1976

System Safety in Rail Transportation

Quave Norvell Smith
University of Central Florida

SYSTEM SAFETY IN RAIL TRANSPORTATION

BY

QUAVE NORVELL SMITH
B.S.I.E., Louisiana State University, 1971

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Engineering
in the Graduate Studies Program of
Florida Technological University

Orlando, Florida

ACKNOWLEDGEMENTS

I would like to express my appreciation to those persons which without their assistance this thesis could not have been completed. The members of my graduate committee, Dr. Christian S. Bauer, Dr. John D. Dennis, and Mr. Benjamin W. Lin, whose comments and suggestions led to the successful completion of this thesis. I would also like to express my sincere gratitude to my chairman, Dr. George F. Schrader, for his excellent advice, encouragement, and helpful criticisms.

SYSTEM SAFETY IN RAIL TRANSPORTATION

by

QUAVE NORVELL SMITH

ABSTRACT

This thesis, "System Safety in Rail Transportation," is addressed to an individual having a basic technical background but little or no experience in this field. The thesis discusses the need for and the benefits to be obtained by using system safety techniques and principles in the railroad industry. Examples of typical railroad accidents are reviewed, and it is pointed out that analysis of the hazards in the railroad industry prior to the accidents would have identified problems which eventually resulted in the accidents. The system safety approach, which was developed for use in the aerospace and aviation fields, has proved to be extremely effective and is now being adapted to many other areas. The surface modes of transportation have the greatest need for these techniques. The techniques covered in this thesis include Hazard Analysis, Fault or Logic Tree Analysis, Failure Modes and Effects Analysis, and Probabilistic Cost Analysis. The thesis also describes a hypothetical model for organizing and implementing system safety approaches in an existing railroad company.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure

I. OBJECTIVE AND PROCEDURE

Rail transportation safety is the end product of many interrelated efforts. Management decisions and operating policies must reflect a new concern for safety. Many occupations must integrate new concepts and new skills. Those engaged in equipment design, safety training, establishing maintenance standards and operating policies, using equipment, inspection and compliance procedures, establishing and enforcing standards and safety regulations, as well as safety managers, government administrators and safety program managers, must all be cognizant of a body of knowledge which includes appropriate safety considerations.

This thesis "System Safety in Rail Transportation", was initiated as a result of an effort by the U. S. Department of Transportation and the Transportation Systems Institute of Florida Technological University to conduct a research project concerned with the analysis of manpower requirements in transportation safety. The research project is a follow on to recommendations made during a workshop on transportation safety held in November, 1972.

The objective of this thesis is to develop a conceptual model of a system safety program and organization structure for an existing railroad involving the following elements:

1. Review of the magnitude, trends, reporting criteria, cost of accidents, and customer

attitude in the railroad industry.

2. Review of safety regulations.
3. Review of the "state-of-the-art" in system safety.
4. Development of a hypothetical model for system safety in rail transportation.
5. Examples of system safety techniques applied to the railroad industry.

As can be determined very little has been done along the lines of applying the principles of system safety to the operations of railroads. This thesis is not expected to solve the problem, but to explore and consider such system safety programs and techniques that would enhance the accident and fatality problem in the rail industry. It is recognized that these initial efforts only serve to open the door. It is realized that more comprehensive research is needed.

In addition to discussing the need for system safety, this thesis also looks at the benefits to be obtained by using system safety techniques in the railroad industry. It is pointed out that analysis of the hazards in the railroad industry prior to the accidents would have identified problems which eventually resulted in the accidents.

The system safety approach encourages visualization of the interrelationships of all the components of railroading and brings accident possibilities into focus automatically in an orderly

manner. Its effect is to broaden the application of safety from a piecemeal problem solving exercise to a safely designed opration.

II. OVERVIEW OF THE INDUSTRY

A. Magnitude

Although it is beset with many problems, the railroad industry in the United States continues to play a significant role in the movement of people and goods throughout this nation. The sixty eight Class I railroads and their nearly one third million miles of track serve every major city in the country.

The United States has about 28 percent of the worlds' railroad mileage and handles about 24 percent of the freight that moves on the railroad of the world. The combined freight capacity of all the railroad cars in the United States totals over 119 million tons. The average freight train carries over 1,800 tons of freight in 70 cars.

Total railway mileage has decreased about 46,000 miles since 1920, but railroads carry more than three-fourths again as much freight today as in 1920.

Railroads in the United States represent an investment of more than $37 billion. About 52 percent of this investment is in fixed property. About 48 percent is in rolling stock. Over 530 companies comprise the railroad system of the United States. Freight accounts for about 90 cents of every dollar of income earned by the U. S. railroads.

In terms of overall progress, the American railroads are,

for the most part, continuing to improve their position both operationally and financially within the total spectrum of transportation activities. The Year 1972 appeared to be somewhat of a pivotal year in this regard with operating revenues reaching a record high of $13.4 billion. Freight traffic volume and freight revenues were on the upswing, but so were expenses. The rate of return on net investment was 2.95 percent.

On the merger front, the Illinois Central and Gulf Mobile and Ohio finally joined forces by mid-year after a string of court cases.

The industry's candidate for the longest-running labor dispute, the Fireman-Manning case, was finally settled. Also, studies of the Railroad Retirement System paved the way for settlement by 1973.

Railroads made significant progress in getting attention for legislative proposals. However, the Surface Transportation Act, which looked like it would put railroads on an equal footing with other carriers, disappeared with the 92nd Congress.

The transportation spotlight in 1972 was on the rail movement of export grain. Spurred by a 17.6 percent increase in grain carloadings in the final six months of 1972, the nation's major railroads achieved an all-time record in freight traffic for one year - 7.78 billion ton/miles. Heavy grain movements continued into 1973 and, in the first four months, carloadings of grain were up 37 percent over 1972. All rail traffic, in fact, increased

8.5 percent in ton/miles as compared with the same period of 1972. The increased demand for freight service was expected to continue throughout 1973.

The speed of the trains vary from 10-15 miles per hour on Class I track to 110 miles per hour on Class 6 track. The average speed for passenger trains is 41 miles per hour and 21 miles per hour for freight trains.

B. Trends

Throughout its history, the railroad industry has maintained a reputation as a safe method of transportation. In recent years this reputation has been tarnished by many publicized accidents involving the older systems. However, with the exception of water transportation, the fact clearly remains that passengers or freight on board a train have not been subjected to the incidence of fatality or freight loss associated with other modes of transportation.

As seen in Figure 1, railroad accidents have increased steadily since 1964, from 5,317 to 10,419 in 1974. However, railroad fatalities have decreased from 880 in 1964 to 689 in 1974.

Preliminary statistics for calendar year 1974 show that train accidents increased from 9,698 in 1973 to 10,419 in 1974. However, the rate of increase in train accidents in 1974, was lower than in the previous year. The 1974 increase is estimated at 7.4 percent.

Statistics for the year 1974 indicate that injuries to railroad employees on duty were 15,641, compared to 13,098 for 1973.

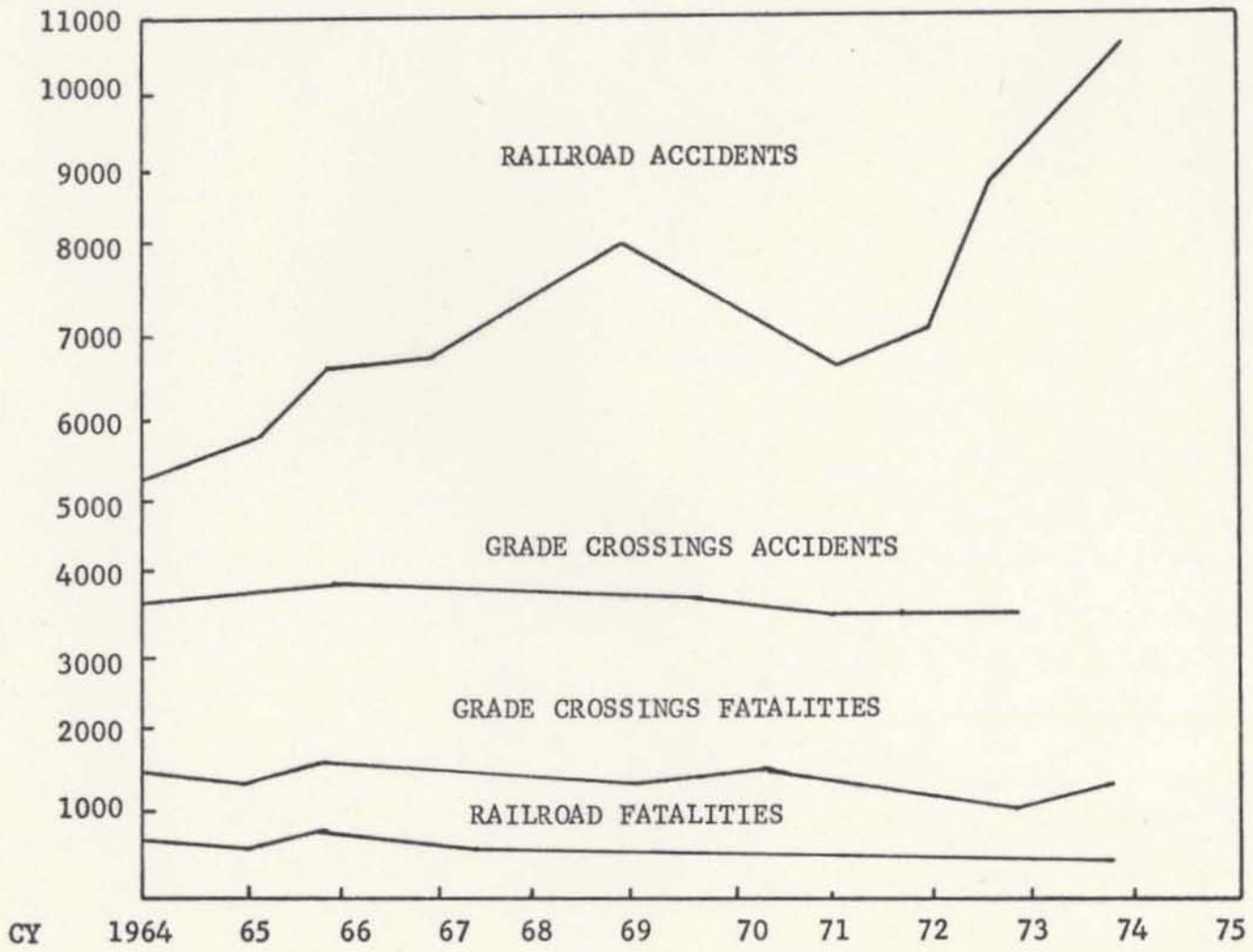


Fig. 1. Railroad Accidents and Fatalities

Fatalities to railroad employees on duty declined from 158 in 1973, to 140 in 1974. Casualties in grade crossing accidents declined from 3,306 in 1973 to 3,275 in 1974. For 1973, the rail industry suffered 0.07 passenger fatalities per 100 million passenger miles while passenger fatalities on buses were 0.24, domestic airlines 0.10, and automobiles and taxies were 1.70 (1). In terms of employee safety, the rail industry compares favorably with other heavy industries.

C. Reporting Criteria

Statistics in this report are based on a monetary reporting threshold which involves train accidents of $750 or more damage to equipment, track or roadbed, and personal injury. The personal injury includes accidents which incapacitates a person from performing acceptable the duties assigned to him.

Effective January 1, 1975, the reporting criteria were revised in order to correct the distortion that has occurred over the years in the statistics relevant to reportable train accidents due to inflation. The criteria for reportability in the personal injury category have also been revised to be comparable with the Department of Labor's Occupational Safety and Health Act requirements.

A new reporting threshold, which will be reflected in the 1975 reports, is for $1750 in damages to railroads on track equipment, signals, track, track structures, and roadbed. This monetary threshold will be adjusted every two years in increments of $100 to reflect inflation pertinent to railroad train accidents. The 1975

criteria for reporting of personal injuries define "Reportable" as being any event arising from the operation of a railroad which results in medical treatment, restriction of work or motion, loss of workdays, loss of consciousness, or any occupational illness of a railroad employee as diagnosed by a physician (2).

D. Cost of Accidents

The major causes of accidents are human factors, equipment, and track. Associated with each accident is a damage cost. The average damage cost related to accidents, as a result of human factors was $12,337, defects in equipment was $21,360, and defects in way and structures was $16,225. The total cost of damages for the 10,419 accidents reported in 1974 was $175,354,810. This averages to $16,830 per accident.

For 1974, track defects caused 41 percent of accidents, equipment defects caused 20 percent while human error caused 20 percent.

Existing track standards cover 98 percent of the reported causes of all track accidents. Therefore, it appears obvious that the major effort in the track area must be to obtain better compliance with these regulations. This means better inspection and compliance actions by the railroads themselves and the identification of trouble areas by Federal Railroad Administration and State track inspectors. Recently adopted equipment regulations cover 97 percent of the equipment defects causing train accidents. Again, a major effort must be made to obtain better compliance with equipment

standards (1).

E. Customer Attitude

According to Nick Thimmesch, a Washington editor writing in the Orlando Sentinel, the ride is getting bumpier and bumpier over most of the nation's railway roadbeds and tracks (3). Train derailments have been increasing over the past few years even though injuries and deaths are fewer from train accidents. Nearly all derailments are freights. The resultant economic loss in the past 10 years is about $1 billion. The potential damage is even greater because freights haul increasingly large shipments of hazardous materials, like propane and vinyl chloride.

Rail passenger fatalities per 100 million miles are substantially lower than airlines and buses, and far lower than auto travel. Still, derailment, the number one cause of train accidents, presents a serious problem and broken rails are caused by poor maintenance. Poor maintenance results when railroads are broke, which many of them are.

The Interstate Commerce Commission authorized a 10 percent rate increase in June 1974 with the provision that railroads perform postponed maintenance. But better rail days are coming. The bankrupt railroads will soon get several hundred million dollars in guaranteed loans and subsidies from the U. S. Government to improve track and equipment. The United States has the technology and the need for a better railroad system.

III. REVIEW OF SAFETY REGULATIONS

For almost 50 years after their beginning, railroads in the U.S. were subject to little governmental regulation. Regulation at first was largely at the state level, but public sentiment resulted in the passage in 1887, of the Interstate Commerce Act, which placed the railroads under federal regulation. Later, other acts broadened and extended the areas of federal regulation so that the railroads finally had to clear through the Interstate Commerce Commission almost all proposals for changes in such matters as financing, equipment standards, signaling and rates.

With the establishment of the U.S. Department of Transportation (DOT) on April 1, 1967, administration of nine rail safety laws previously administered by the Interstate Commerce Commission (ICC) was transferred to the Federal Railroad Administration (FRA). Thus, the Federal Railroad Administration is now responsible for the administration of the Safety Appliance Acts, the Ash Pan Act, the Locomotive Inspection Act, the Accident Reports Act, the Signal Inspection Act, the Hours of Service Act, and the Transportation of Explosives and Other Dangerous Articles Act, all with respect to railroad transportation (1).

The Federal Railroad Safety Act of 1970, gave the Secretary of Transportation authority to regulate all areas of railroad safety. The Secretary delegated this authority to the Federal

Railroad Administration. The task is complex, and FRA's initial efforts were directed toward the adoption of track and equipment standards. Through a number of studies, FRA is now developing both a short term action plan and a longer range plan to provide a basis for directing the federal safety program.

In addition to the Federal Railroad Safety Act of 1970, the FRA also has the legislative authority granted under the Rail Safety Improvement Act of 1974. These acts provide for an effective safety program with a combination of research, regulations and enforcement.

There are now eight states participating in the rail safety track program. They are; Illinois, Iowa, Missouri, Nebraska, Oregon, Pennsylvania, Vermont, and Washington. These states are engaged in the performance of investigation and surveillance activities. A state may participate in this program if the regulations and safety practices applicable to railroad facilities, equipment, rolling stock, and operations are regulated by a state agency. This agency, usually the State Department of Transportation or the State Public Service Commission, must submit an annual certification.

State participation regulations require state track inspectors to meet the same qualifications as their federal counterparts. However, this program has been hampered in expanding participation to a greater number of states chiefly because of the prescribed inspector qualifications. Few states already employ inspectors with sufficient track experience, and, because of the lower level of state salaries, some states have not been able to recruit qualified

candidates.

According to the Railroad Safety Act of 1970, laws, rules, regulations, orders and standards relating to railroad safety shall be nationally uniform to the extent practicable. A state may adopt or continue in force any law or regulation until the Department of Transportation has adopted a rule or law to cover the subject matter of the state requirement. A state may also adopt or continue in force an additional or more stringent law or regulation when necessary to eliminate or reduce an essentially local safety hazard, when not incompatible with any federal law, and when not creating an undue burden on interstate commerce.

The National Transportation Safety Board (NTSB) has the authority to determine the cause or probable cause of conditions and circumstances relating to accidents. This authority may be delegated to any office or official of the NTSB or to any office or official of the Department of Transportation.

In a system that is dependent heavily upon fulfillment of special procedures, it is essential that action be monitored to ensure compliance with those procedures. One prime prerequisite for monitoring procedures or rules is to establish rules that distinguish compliance or non-compliance before an accident occurs. If a rule is unforceable, it is of little value in controlling safety.

IV. STATE-OF-THE-ART IN SYSTEM SAFETY

In the beginning as with every new discipline the System Safety pioneers struggled to develop an acceptable definition of "their thing." Years later, although many definitions have been "coined" a standard simple, understandable definition eludes us.

One definition of "System Safety" is the optimum degree of hazard elimination and/or control within the constraints of operational effectiveness, time and cost, attained through the specific application of management, scientific and engineering principles throughout all phases of a system life cycle (4).

During the 1960's several appraoches to System Safety Programs were tried all of which proved to be inadequate. There was some effort to quantify safety requirements by specifying accident probabilities and requiring a demonstration of these probabilities by analysis.

Although system safety was developed primarily as a risk management tool for complex aerospace systems, the logic and techniques developed have many applications for non-aerospace products and systems. To achieve the goal of complete safety -- the freedom of risks of injury or loss of equipment or property -- is impractical. It is practical however, to try to approach this goal not only for moral reasons but also for cost effectiveness. This definition of practical approach and assurance of acceptable

risks is the primary business of system safety. Briefly, this is accomplished by translating prior safety experience, engineering analyses, safety research and management actions into a stated acceptable risk of injury or loss of material.

System Safety techniques, as developed and employed on weapon systems and space projects can unquestionally be used advantageously in the design and manufacture of any product and in any industry. The trick is to select those system safety features which are compatible with the product line or industry and apply them effectively without compromising ability to compete in the market. In other words the cost of the system safety application, and its predicted impact on cost, performance, and service must be accurately predicted if it is to be successful. At the same time, results must be answered which provide reasonable measures to minimize the risk of injury or damage to persons or property, giving full regard to applicable industry standards, regulatory requirements, technological developments, and the standards of care required by society.

The advantages of the new technology "System Safety" have been demonstrated in aerospace, aviation, and military activities. Basic principles used in "System Safety" include the analysis of system to identify hazards and the adoption of methods to eliminate or control those hazards. Many management and engineering methods currently in use in the aerospace and aviation industries are being adopted for use in other areas. However, the procedures of analysis under the concepts of "System Safety" have not as yet been adopted

in the surface modes of transportation.

An accident cause is, in actuality, an extension of a hazard to its potential. The term "hazard" is preferred as it is not difficult to visualize man as an accident cause, but to categorize man as a hazard places a different perspective on the interpretation. It is easy to dismiss an accident as resulting from an employee's negligence, when in fact, the accident may have resulted from the failure of the system.

The railroad safety system, like all other systems, includes four components: (a) management, (b) man, (c) machine and (d) media (environment) (5). The Ven diagram in Figure 2 illustrates the interface of these components for the safety of the railroad system. It should be noted that the safety factors involving man's performance in the system cannot stand alone, but must be interfaced with management, machine, environment, or various combinations of each or all. A man-failure must involve a system failure in a safe system.

It is impossible or uneconomical to eliminate all hazards in the railroad system, but other choices are available. If the hazard presents a risk that cannot be assumed economically or sociologically, the system must be made tolerant to the hazard. This can be done by three methods.

The installation of safety devices that do not require human intervention to function is the preferred method of making a system tolerant to a hazard. A second method of making a system tolerant

to hazards involves the installation of warning devices. These devices are less reliable than safety devices as they require human intervention to respond to the warning given. The third method of making a system tolerant to hazards involves the establishment of special procedures such as operating rules, bulleting, or special instructions. For the most part, the safety of the railroad system, as we know it, is dependent largely upon this method. As one would expect, the preferred method of making a system tolerant to a hazard also is generally the most expensive. The initial cost of the three methods generally varies directly with their effectiveness.

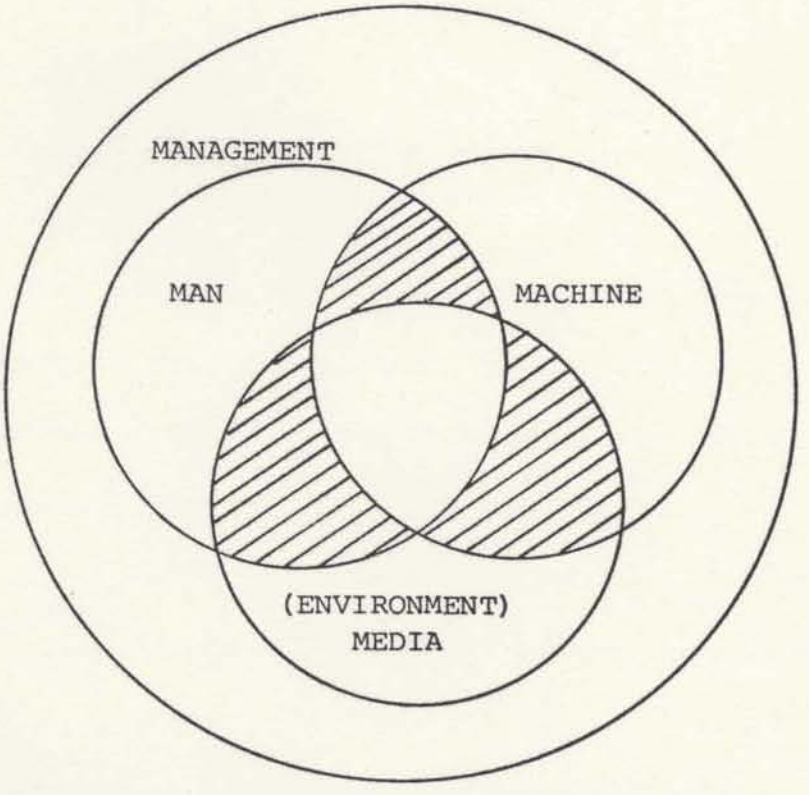


Fig. 2. Interrelationship of Safety Factors

V. HYPOTHETICAL MODEL PROGRAM FOR SYSTEM SAFETY IN RAIL TRANSPORTATION

A. Introduction

In order to clarify the safety activities in the rail transportation industry, the following is set forth as a basic program model to clearly establish its operational effectiveness in the industry. It consists essentially of an outline of the relationships of management and employee responsibilities which are necessary for this type of safety program.

It is felt that this model should become a basic part of management policy and help govern its judgment on matters of operation equally with considerations of types of service offered, budget distribution, personnel relations, and other phases of management policy.

This model program is administered, upon approval, by the assistant vice-president of system safety. His primary purpose is to assist management in the recognition, elimination and/or control of hazards particular to that industry.

Table 1 depicts the hypothesized System Safety and Operations Department Operational Control Modules in each of the eight sub-department groupings. Functionally similar modules, such as security and property protection, are aligned horizontally in the figure. Operational Control modules consist of those routine

TABLE 1

SYSTEM SAFETY AND OPERATIONS (HYPOTHETICAL) MODULES IN A RAILROAD COMPANY

	SYSTEM SAFETY AND OPERATIONS FUNCTIONAL ACTIVITIES							
	SYSTEM SAFETY				OPERATIONS			
SUB-DEPARTMENTS / FUNCTIONS	SECURITY & PROPERTY PROTECTION	INSURANCE & HEALTH CARE	FREIGHT DAMAGE	PERSONAL INJURY PREVENTION	TRANSPORTATION	ENGINEERING & RESEARCH	LOCOMOTIVE & TRACK MAINTENANCE	SIGNALS & TRAIN CONTROLS
INTERPRET NEEDS		X		X	X	X	X	X
INTERPRET LAWS		X		X	X	X	X	X
PROGRAM PLANNING & DEVELOPMENT	X	X	X	X	X	X	X	X
PROGRAM ADMINISTRATION	X	X	X	X	X	X	X	X
SAFETY ANALYSIS & DESIGN				X		X	X	X
INSPECTION & COMPLIANCE	X			X			X	X
ACCIDENT INVESTIGATION				X				
ENFORCEMENT & SECURITY	X							
TRAINING	X			X			X	X
OTHER SAFETY SERVICES		X	X			X		
SCHEDULING & ROUTING	X		X	X	X		X	X
INVENTORY & EQUIPMENT CONTROL							X	X
MAINTENANCE							X	X
OPERATING PRACTICES					X			
CLEARANCE CONTROL						X		
CROSSING PROTECTION						X		X
ENVIRONMENTAL CONTROL						X		

activities carried out by the sub-department as shown vertically in the figure. A check in the column under the sub-department indicates that the function that is aligned horizontally with it is performed by someone in that particular sub-department (6).

B. Purpose

The first step to developing a System Safety program is to determine needs of the industry, employee, and customer. To start with, this can be rather vague. However, this is an iterative process and further iterations will result in necessary specifics. To state that the program will make the system safe gives little idea of what it is to do. To state that the program will reduce, to an acceptable level, the possibility of accidental personnel or passenger injury, equipment, freight, or facility damage which could result in significant loss, gives a little better idea of why the program is there and what the program goals are.

The management of rail transportation companies hold in high regard the safety, welfare, and health of the public and their employees. The System Safety and Operations Department in this hypothetical model was organized for the purpose of grouping under the administration of a vice-president, the safety and operations related functions previously being performed in the operating, finance and law departments. Specifically the following functional groups comprise the Systems Safety and Operations Department: Security and Property Protection, Health Care and Insurance, Freight Damage Prevention, Personal Injury Prevention, Transportation,

Engineering and Research, Locomotive and Track Maintenance, and Signals and Train Controls.

The reason for organizing the safety related functions was the need to develop a closer degree of coordination and cooperation between related activities, directed toward the goals of (a) reducing the human suffering and expense of personal injuries, and (b) the expense and customer dissatisfaction related to freight loss and damage. Too often, the responsibility for achieving these goals have been to widely distributed. Not only should this model be more effective, but also, labor savings should be realized. In recognition of this and in the interest of modern management practice, this model will constantly work toward the following safety goals:

A. Identify safety - critical systems, subsystems, components events, and operations.

B. Produce meaningful design, operation, and training criteria to control identified hazards.

C. Define acceptable risks and provide trade-off guidance.

D. Verify that safety design criteria have been met and/or provide guidance for trade-off decision.

E. Examine the system and its life cycle to identify possible hazards.

F. Provide management with visibility of efforts to control hazards.

These goals will be realized by performing the following ten

basic safety functions:

1. Interpretation of needs
2. Interpretation of laws
3. Program Planning and Development
4. Program Administration
5. Safety analysis and design
6. Inspection and Compliance
7. Accident investigation
8. Enforcement and security
9. Safety training
10. Other safety services.

These basic safety functions are shown in Figure 3.

C. The Information Network For System Safety

The safety information network is only one of the several kinds of networks found in railroad organizations; other systems include money, personnel, work orders, and capital equipment networks. The system safety specialist, in laying the groundwork for the segmental development of a properly integrated system, must go beyond a monolithic conception as shown in Figure 4. He must recognize that not all information processes are equally strongly tied together in the company. This is a basis for initial subdivision of the universe of information processing in the company into conceptually manageable parts.

This problem is multidimensional. If Figure 4 is reviewed, it can be shown that certain functions such as inspection, and

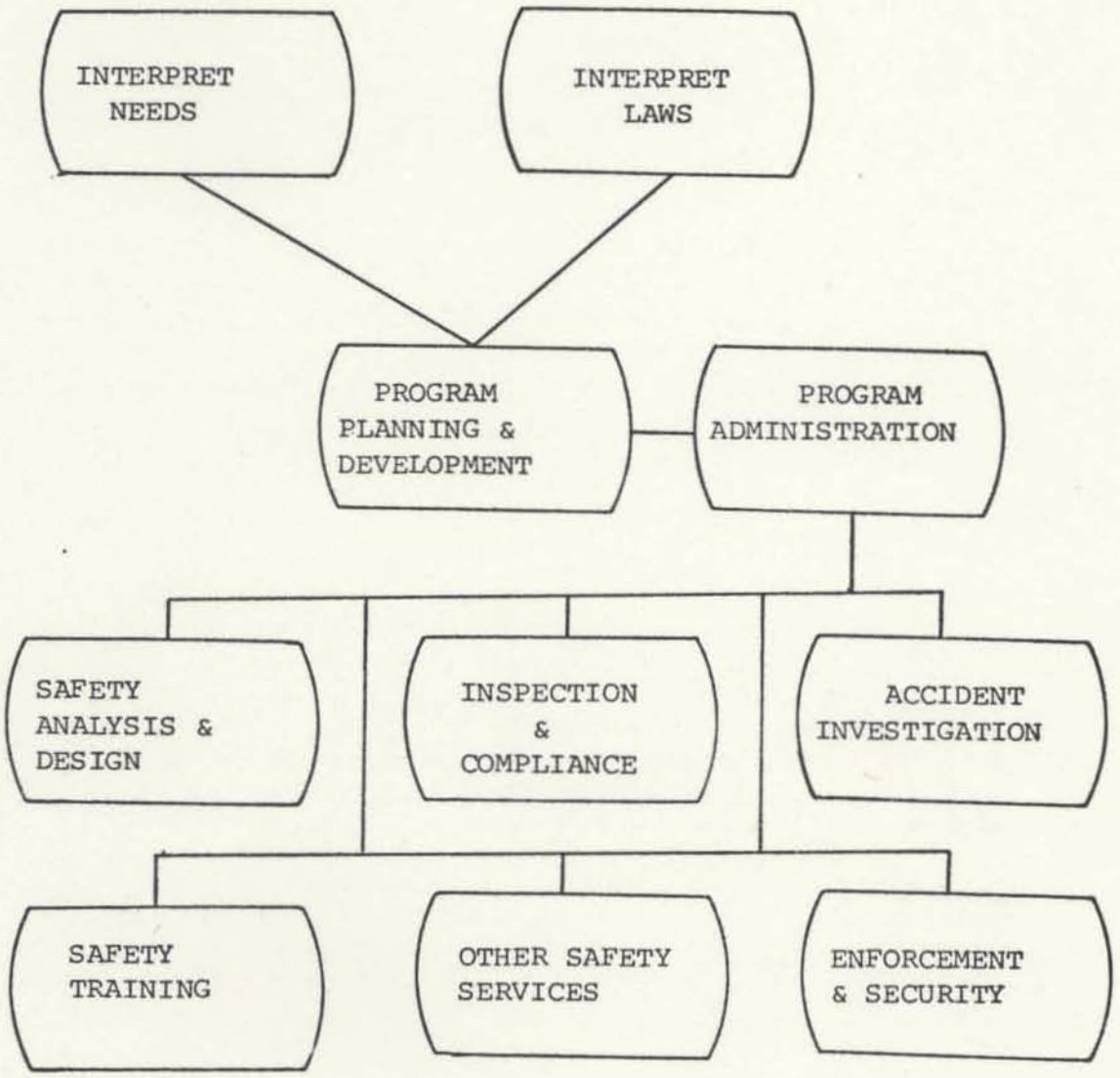


Fig. 3. Railroad Transportation Safety Functions

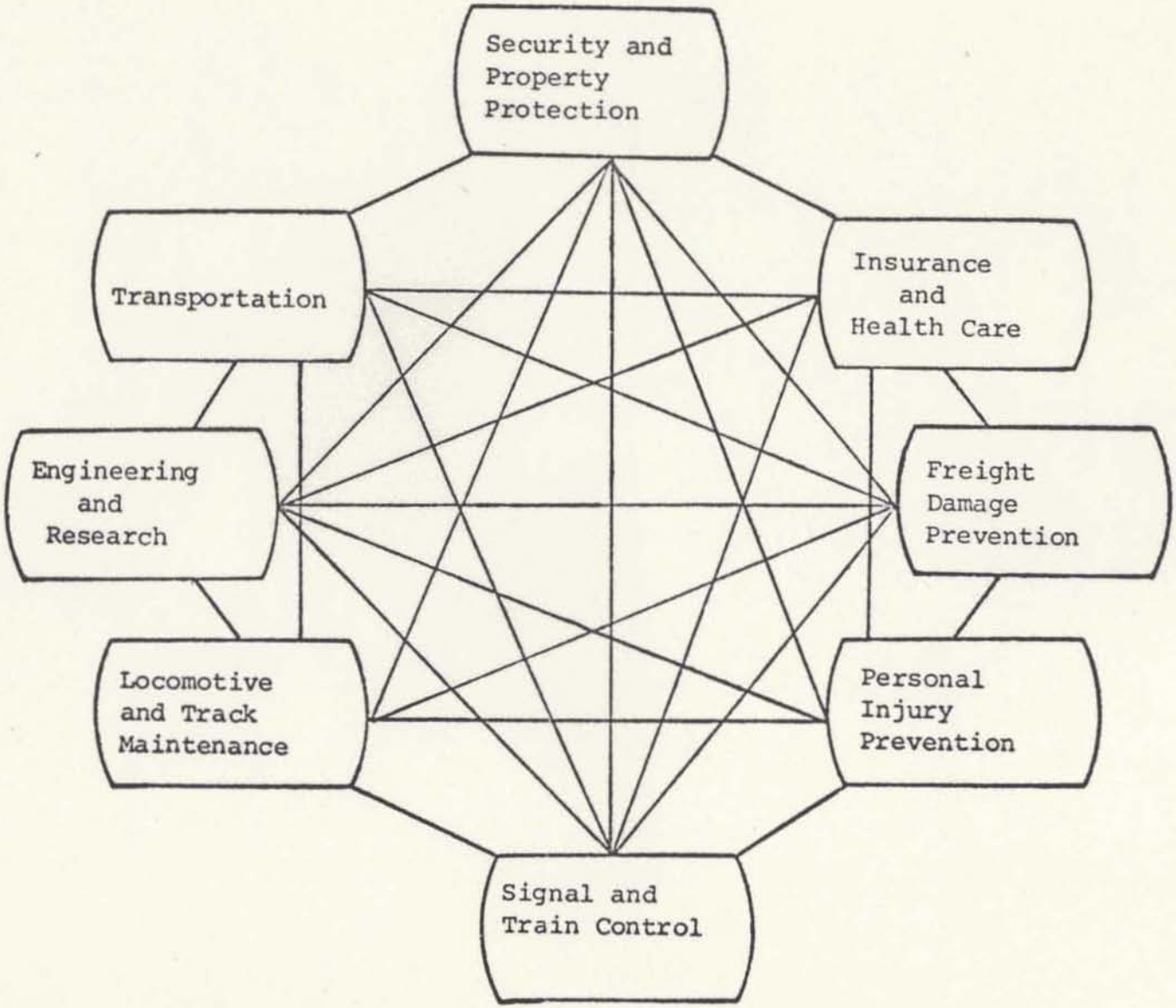


Fig. 4. The Systems Approach To Organization and Information Flow

compliance, accident investigation, safety training, etc., occur in more than one network. Therefore the view may be adopted, that networks should be organized along the lines of similarity of activity, regardless of the functional loci of parts of the activities.

It has been postulated that two kinds of information systems exist; major (one that affects the entire organization), and minor (not of minor importance, but one that applies only to a limited part of the organization) (7). The major safety information systems are inspection, hazardous materials, historical data, new technology, accident, and injury, operational hazards reports, external compliance directions, and catastrophic situations.

Planning is the most basic of all the safety functions because it involves the selection of organizational and departmental objectives and the determination of the means to achieve these objectives. Essentially, planning is the same whether applied to an entire organization or to any hierarchical level in it. Planning generally involves five steps or processes as seen in Figure 5. They are:

1. Recognizing hazards or unsafe situations.
2. Defining problems or unsafe situations and developing alternate courses of action.
3. Making a decision.
4. Implementing the plan
5. Checking control performance against the plan

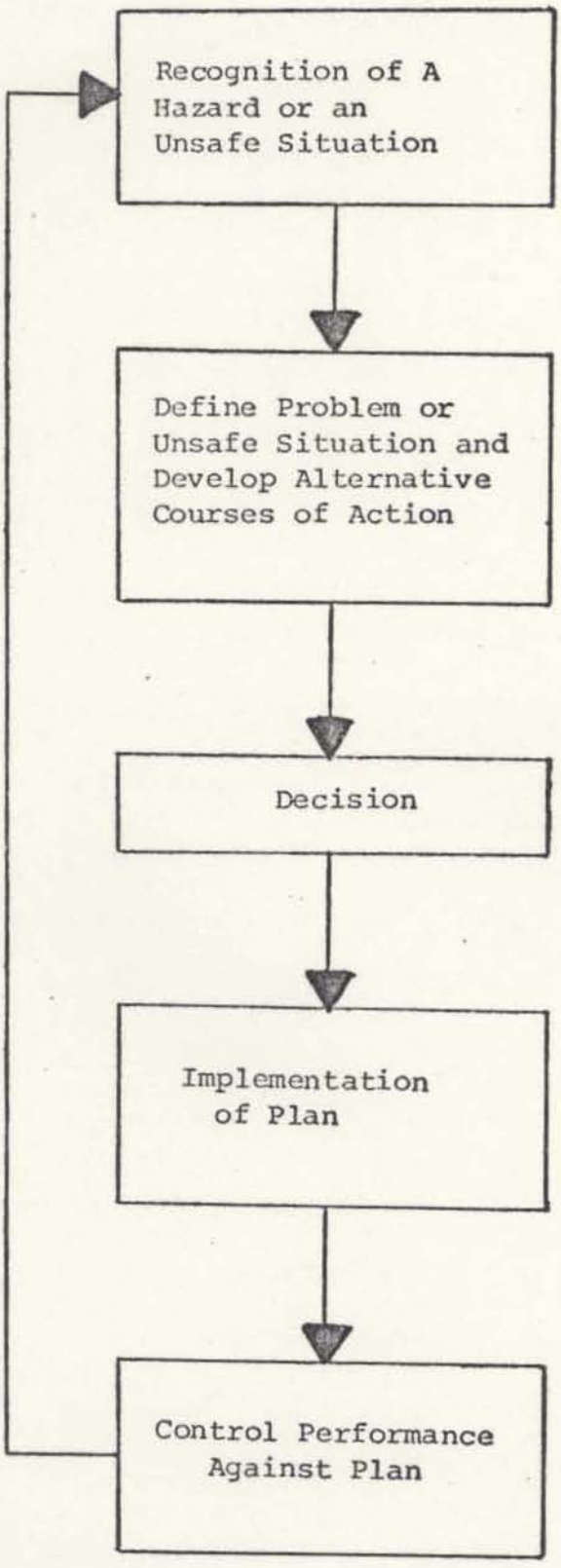


Fig. 5. Major Steps in System Safety Planning

Now that the networks have been discussed, the conceptual flow of information will be reviewed. As seen in Figure 6, no matter what type of information is fed into the system, the flow process is basically the same. A piece of information is analyzed, investigated, and some form of action is taken. The results of this process is then fed back into the system.

The information sources of the system safety department can be classified into three broad types; (a) environmental, (b) competitive, and (c) internal (8). The environmental information consists of;

(a) governmental policies

(b) economic trends

(c) technology

(d) factors of operation

The competitive information includes such things as;

(a) industry demand

(b) firm demand

(c) competition - past, present, and future

Often internal premises affect the planning and operating decisions of the safety department more so than external information. As they relate to the total system safety process they are;

(a) policies

(b) financial plans

(c) investigations and inspections

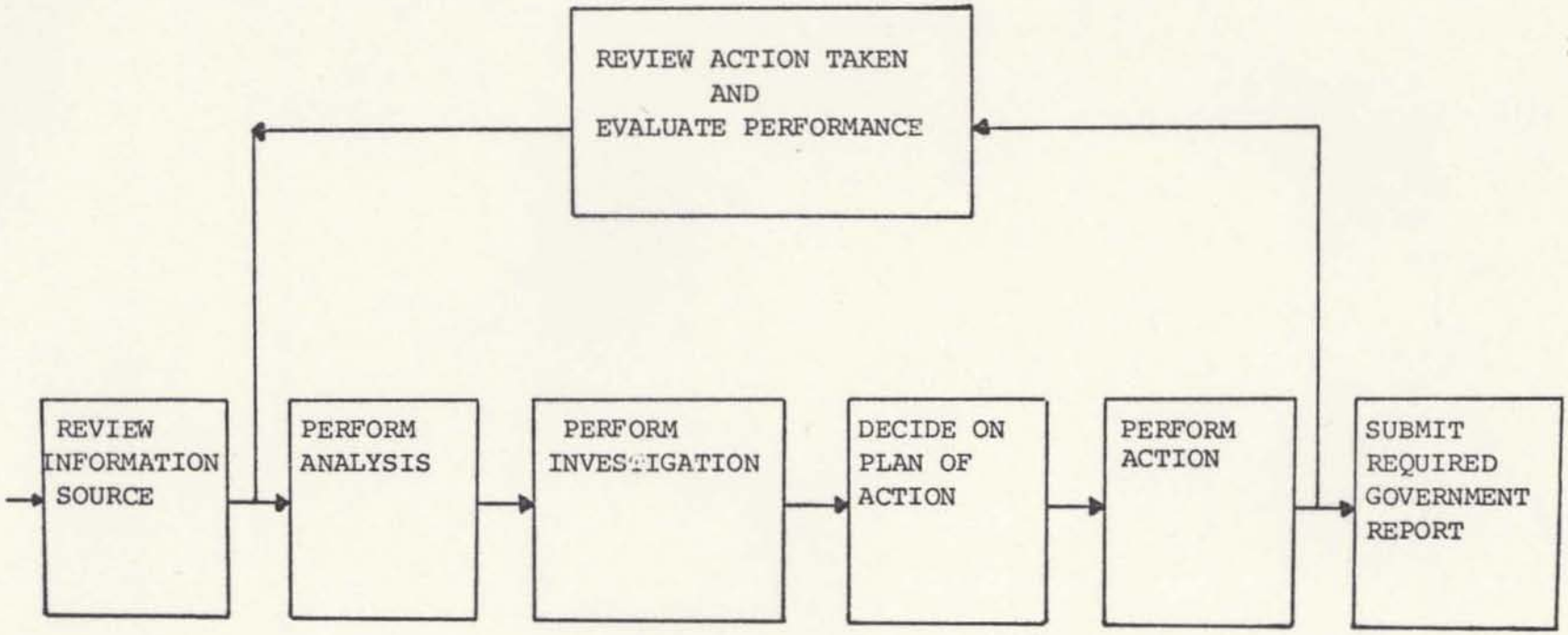


Fig. 6. Conceptual Information Model of System Safety Department

It was previously shown that the conceptual operations of the system safety department could be defined in terms of the elements and properties of information source (input), analysis, investigation, and action taken (output), and in a strict sense this is so. However, this system is dynamic and changes inevitably occur. Moreover, in this dynamic system it is necessary to review, periodically or continuously, the state of the output in order to make necessary alterations because of changes.

It is important to understand how the elements of the safety department function as a system because, like any other system, the department operates through the medium of information.

The conceptual system flow chart as seen in Figure 6 is a common method of indicating the general structural of an information system. This system flow as illustrated by the flow chart, is quite general in nature and indicates only the main components of the system. At this stage, the chart does not indicate what processing occurs at particular steps in the flow or what specific data, equipment, or personnel are involved. However, the chart is extremely important because it provides the foundation and framework upon which detailed specifications will follow.

D. Organization For System Safety

The system safety concept is the elimination of hazards in the system. This is the most economical way to reduce accidents which result in loss of life and property. System safety not only

identifies hazards, but also shows the likelihood of their activation and points out the alternative methods available to eliminate them. With this visibility into the problem area, management can then decide which hazards to eliminate, which hazards to control, and which risk to assume.

The activities of hazard recognition and elimination or control encompass the sum total of Accident Prevention. If these activities were perfectly achievable all else could be disregarded and supplemental activities would not be necessary. Since they are not perfectly achievable, the goal must be to first accomplish them in the best way possible and then apply supplemental management and technical resources to enhance the desired level of safety.

These activities are the responsibility of every director as shown in Figure 7. The general hazards associated with rail transit are readily determined from inspections, investigations, and the Federal Accident Statistics. This organizational structure permits flexible and efficient response to the rail industry's safety and operation needs. This structure affords the department the mobility and exposure necessary to carry out its programs.

To carry out the responsibilities assigned the System Safety and Operations Department as seen in Figure 7, the department is composed of staff and field personnel. The staff personnel provide the general direction to all accident prevention programs as well as to the administrative matters of the department. Field personnel carry out safety programs in the field as well as preparing

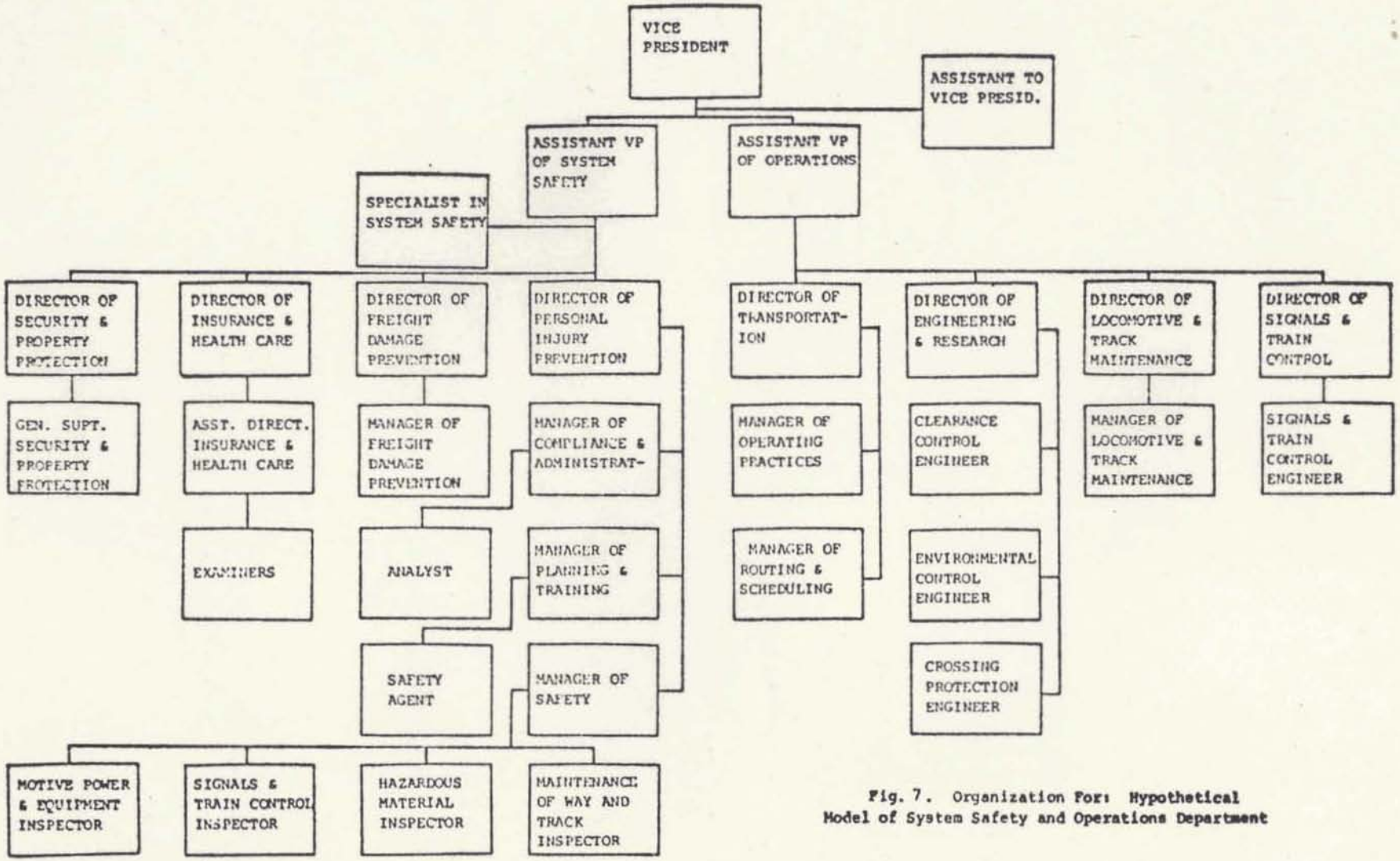


Fig. 7. Organization For: Hypothetical Model of System Safety and Operations Department

reports of investigative activities.

E. Responsibility

The system safety organization shall be responsible for managing and performing the overall system safety program. The responsibilities and functions of those directly associated with system safety policies and implementation of the program shall be clearly defined in this section.

Ideally, it should be possible for any given mode of transportation to describe a unique system safety organization which would be optimal for carrying out a safety program suitable for that particular mode of transportation. From a practical point of view, it is obvious that no such single organizational entity can be described. However, it can be stated, that all of the task in the domain of safety which need to be performed so that a system may be operated safely can always be specified. It can further be stated that there are usually a variety of ways to organize so that these tasks will be performed satisfactorily. The job descriptions that follow are only one way to accomplish the tasks necessary to operate a railroad safely.

Job Title

Vice President

Scope

The Vice-President of the System Safety and operations department has the responsibility to develop an effective program of accident prevention.

Job Title

Assistant to Vice President

Scope

The Assistant to Vice President serves as an administrative assistant to the Vice President. He makes recommendations concerning policy in administrative, personnel, and other matters pertaining to the eight sub-departments in the System Safety and Operations Department and is directly responsible to see that all administrative policies and directions are carried out by these groups to achieve the mission of reducing safety losses.

Duties

1. Responsible for the effective administration of all offices in the department, which includes all record keeping, reports, payroll, requisitions for and repairs to office equipment, assignment of leased vehicles and personnel.

2. Supervision of office clerical force, bulletining and assigning contract-covered positions.

3. Serves as departmental personnel officer, and supervises the preparation and maintenance of personnel records, preparation of authority for payroll changes and submits them to the sub-department heads for approval. Makes recommendations regarding promotions and merit increases.

4. Prepares the staff departmental budget and coordinates the preparation of budgets by the sub-departments. He also constantly keeps a close check on expenditures and brings to the attention of the sub-department heads those areas in which expenses are unnecessary or out of line.

5. Administers labor agreements, investigates and replies to claims and grievances and prepares recommendations for handling by labor relations.

6. Prepares directives pertaining to activities of the various sub-departments and replies to correspondence received by the department head.

Job Title

Assistant Vice President for System Safety

Scope

Assistant Vice President for System Safety under the overall direction of the Vice President, exercises general supervision over the four sub-departments comprising the system safety group. Establishes yearly objectives for each of the sub-departments as well as periodic goals for progress which must be achieved during the year. Monitors progress, and initiates corrective action when indicated, to assure that all departmental and sub-departmental goals are met on schedule. Makes policy recommendations to the Vice President, also has direct responsibility for implementation of all departmental programs and policies.

Duties

1. Under the overall direction of the Vice President, supervises the activities through department directors, of the four sub-departments comprising the system safety group.

2. Responsible for continuous appraisal of functions performed by each group and of devising methods of eliminating non-productive functions or, in the alternative, of improving their effectiveness to insure that all goals are met on schedule.

3. Periodically reviews organizational structure of each sub-department to be certain that it is properly designed to perform the responsibilities assigned to it.

4. In consultation with sub-department directors, evaluates personnel to ascertain their effectiveness in the positions to which they are assigned, and to determine which individuals are capable of taking on increased responsibilities as well as those whose responsibilities should be reduced.

5. Consults with personnel of other railroads, and industrial concerns to find better methods of reducing or eliminating safety losses.

6. Works closely with other departments to assist in designing and implementing methods and equipment to enable them to carry out their responsibilities insofar as the activities of those departments affect safety losses.

Job Title

Specialist in System Safety

Scope

Specialist in System Safety, reports directly to the Assistant Vice President of System Safety. He is responsible for the development and maintenance of formalized procedures for the analysis of system safety that force a logical examination of all elements of the railroad system and identify all possible sources of accidents.

Duties

1. Identification and classification of all hazards
2. Application of system safety techniques to railroading operations
3. Aid to Assistant Vice President in the development of total system safety program.

Job Title

Director of Security and Property Protection

Scope

Director of Security and Property Protection, exercise general supervision over the Security and Property Protection sub-department. Has direct and immediate responsibility for instituting and implementing programs to prevent theft and damage caused by vandalism and other reasons to property owned by the company and that which is entrusted to its care. Functions as liaison in area of his responsibility with other railroad police departments, federal, state and other agencies. Directs activities concerning the accumulation of data needed to pin point problem areas.

Duties

1. Under the overall direction of the Assistant Vice President of System Safety, administers the affairs of the Security and Property Protection sub-department.
2. Has direct responsibility for the selection, training and overall efficiency of personnel in his group.
3. Develops and implements programs designed to combat thefts, vandalism, trespassing, and other problems.

4. Keeps abreast of industry practices in the area of his responsibility to improve the security and property protection function.

5. Monitors effectiveness of practice engaged in by personnel in his department and make changes where indicated.

Job Title

Director of Health Care and Insurance

Scope

Director of Health Care and Insurance, responsible for developing and implementing health care and insurance programs, that are comparable with the benefits common to the industry.

Job Title

Director of Freight Damage Prevention

Scope

Director of Freight Damage Prevention, exercises general supervision over the freight damage prevention group under the overall direction of the Assistant Vice President of System Safety. Has direct and immediate responsibility for the administration of the group, and for the development and implementation of programs designed to eliminate damage to lading in transit.

Duties

1. Administers the affairs of the Freight Damage Prevention sub-department in the areas of responsibility assigned to it.
2. Has direct responsibility for the selection, training and overall efficiency of personnel assigned to the group.
3. Responsible for the establishment of procedures designed to enable the group to effectively carry out its responsibilities.

Job Title

Director of Personal Injury Prevention

Scope

Director of Personal Injury Prevention, exercises general supervision over the Personal Injury Prevention sub-department under the overall direction of the Vice President of System Safety. Has direct and immediate responsibility for instituting and implementing programs to prevent accidents and otherwise reduce personal and fatal injuries and property damage. Has responsibility for inspection of buildings and facilities to identify and eliminate hazards. Is responsible for compliance with all federal and state statutes dealing with safety. Directs activities concerning the accummulation of data needed in connection with the Federal Railroad Safety Act.

Duties

1. Under the overall direction of the Assistant Vice President of System Safety, he administers the affairs of the Personal Injury Prevention sub-department in the areas of responsibility assigned to it.
2. Has direct responsibility for the selection, training and overall efficiency of personnel in the department.

3. Must develop programs to promote safety and prevent accidents and implement these programs to see that they are carried out efficiently and effectively.

4. Has the responsibility of directing activities to secure and analyze pertinent data concerning causes and effects of accidents.

5. On the basis of data accummulated, must monitor the effectiveness of the programs he institutes and make such changes as seen indicated. Changing old programs and initiating new ones is a continuous process.

6. Must devise plans to meet any emergency situation arising out of a derailment or other accident involving volatile or explosive material and must be certain that those persons responsible for carrying out the disaster plan are adequately trained to meet the situation.

Job Title

Manager of Compliance and Administration

Scope

Manager of Compliance and Administration, serves in a staff capacity under the overall direction of the Director of Personal Injury Prevention, and assists the Director in administering and coordinating the staff and field positions of the Personal Injury Prevention sub-department. Serves as reporting officer to the Department of Transportation and various state commissions in safety, accident related matters. Acts as compliance officer for requirements of federal, state and local regulatory agencies.

Duties

1. Manages the efficient and economical operation of the office of the Director, and assists in the preparation of annual budget and monthly budget variance reports.

2. Supervises the preparation and distribution of all reports, including personal injuries to employees, passengers, tresspassers and others, crossing accidents, etc., to federal and state agencies. Initiates reports to proper parties of all incidents involving hazardous materials to ensure that shipper and carrier errors are connected.

3. Maintains central library for safety regulations, reference materials and literature pertaining to health and safety.

4. Maintains contact and close working relationships with such agencies as the Bureau of Explosives, Department of Transportation, Hazardous Materials Board and others.

Job Title

Manager of Planning and Training

Scope

Manager of Planning and Training, serves in a staff capacity under the overall direction of the Director, and assists the director in coordinating the staff and field functions of the Personal Injury Prevention sub-department. Responsible for developing and implementing programs and training procedures for Personal Injury Prevention activities. Reviews adequacy of safety programs initiated by the department. Responsible for developing management information systems and for analytical reviews of program effectiveness.

Duties

1. Has direct responsibility for developing effective programs and training procedures for Personal Injury Prevention sub-department activities, including operations, visual aids, posters, contests, gimmicks, etc.

2. Analyzes results obtained from the departments safety programs and recommends policies to ensure that programs and procedures are effective and consistent with the objectives of the Operating sub-department as well as the System Safety sub-department.

3. Conducts training sessions for departmental personnel, and makes spontaneous and prepared speeches at safety and staff meetings and civic or other gatherings.

Job Title

Manager of Safety

Scope

Manager of Safety serves in a staff capacity under the overall direction of the director. He has the responsibility for planning, establishing and directing safety, fire prevention, hazardous materials handling and environmental controls programs. The activities of this group must be accomplished through effective implementation of a safety program.

Duties

1. Assists in coordinating the activities of staff and field personnel in the areas of responsibility assigned to the group.
2. Isolates problem areas, develops answers to problems and advises director in safety activities and special safety matters.
3. Recommends standards for personal protective equipment, in consultation with the Operations, sub-department officers and outside experts.
4. Recommends adoption or revision of safety rules and instructions to further personal injury prevention objectivs.

Job Title

Motive Power and Equipment Inspector

Scope

Motive Power and Equipment Inspector, under the direct supervision of the Manager of Safety. Is responsible for the improvement and advancement of railroad safety in areas related to the design, construction, inspection, maintenance and use of railroad rolling stock including motive power equipment, and related appurtenances.

Duties

1. Inspects and tests railroad rolling stock, motive power equipment and related appurtenances.
2. Investigates serious railroad accidents and complaints alleging non-compliance with laws and safety standards.
3. Prepares and distributes reports regarding accidents, potential hazards, and non-compliance with safety laws and safety standards.

Job Title

Signals and Train Control Inspector

Scope

Signals and Train Control Inspector, under the direct supervision of the Manager of Safety. He must implement the department safety policies related to signal and train control systems, insure compliance with laws, regulations, standards and rules relative to the design construction, maintenance, inspection and use of signal and train control systems.

Duties

1. Assist in the review of specifications and plans of the department for rebuilding existing signal or traffic control systems.
2. Investigates serious railroad accidents and complaints alleging non-compliance with the laws and safety standards.
3. Inspects and test signal and train control systems, and components.
4. Prepares and distributes reports regarding accidents and non-compliance with safety laws and safety standards.

Job Title

Operating Practices-Hazardous Material Inspector

Scope

Operating Practices-Hazardous Material Inspector, serves under the Manager of Safety and is responsible for investigating accidents, issuing operating practices, occupational safety conditions, transportation of hazardous material.

Duties

1. Investigates serious accidents and complaints alleging non-compliance with the laws and safety standards.
2. Reviews records to determine whether employees connected with the movement of trains are permitted to be or remain on duty contrary to the provisions of the law.
3. Maintains complete reference library on hazardous materials.
4. Prepares and distributes reports regarding accidents and non-compliance with safety laws and safety standards.

Job Title

Track Inspector

Scope

Track Inspectors serve under the Manager of Safety and is responsible for the improvement and advancement of railroad safety in areas related to the design, construction, inspection, maintenance, and use of railroad tracks and their related appurtenances.

Duties

1. Makes personal inspections to determine the condition of the roadbed, track struction, track geometry, and track related devices.
2. Investigates serious railroad accident and complaints alleging non-compliance with the laws and safety standards.
3. Prepares and distributes reports regarding accidents and non-compliance with safety laws and safety standards.

Job Title

Safety Agent

Scope

Safety Agent, serves under the Manager of Planning and Training, is responsible for having a good working knowledge of the safety and operating rules of the company.

Duties

1. Carry out field inspections aimed at detecting and reporting unsafe work practices, rule violations, conditions and techniques or lack of them posing potential causes for accidents.
2. Personally investigate all lost time injuries
3. Assist in training sessions and seminars for System Safety and other departmental personnel.

Job Title

Analyst

Scope

Analyst, serves under the Manager of Compliance and Administration. He assists in the development, implementation and review of the management information systems used in the System Safety sub-department.

The hypothetical system safety model shall provide a disciplined approach to methodically control safety aspects and evaluate the companies safety activities, identify hazards and prescribe corrective action in a timely cost effective manner. The model will:

a) Evaluate technical approaches to systems safety

b) Identify possible safety interface problems

c) Highlight special areas of safety consideration

d) Define areas requiring further safety investigation

Of course, in addition to the previous basic policy and list of responsibilities there should be descriptions of how safety committees should operate and descriptions of the inspection system to be used.

In conclusion, the first step in system safety is not a technical one. It is concerned with gaining support for the work that follows. The system safety personnel must have the support of most members of the organization in order to obtain information and to obtain acceptance of the final system. At a minimum, members of the organization should be informed of the objectives and nature of the department.

VI. EXAMPLES OF SYSTEM SAFETY TECHNIQUES APPLIED TO RAILROADS

System analysis need not be a highly complicated task. The important point is, given the system description, a decision must be made as to the purpose of the analysis. Once this decision has been reached, the analytical technique that will produce the needed data is selected and applied.

On initial examination, there appear to be many analytical techniques available for the purpose of identifying hazards and evaluating risks. However, a detailed review of these methods will reveal that most of them are modifications of other techniques, and that the modification was made either to accommodate a unique system, or to develop a unique set of data.

There are essentially three basic analytical methods:

1. Hazard analysis
2. Logic tree or fault analysis
3. Failure mode and effects analysis

In the sections that follow, these three methods will be discussed and explained with the use of examples. In addition to the three analytical methods mentioned above, the probabilistic behavior of accident systems will be considered.

The examples given in the sections that follow are only for the purpose of illustrating the application of the foregoing

principles and procedures to typical situations which might be encountered in the rail transportation industry. While they follow good industry practice, they are only illustrations, and must not be regarded as a complete engineering analysis of a specific problem.

The numerical values shown for the probability of occurrence of certain events are assumed for illustrative purposes only and have no basis in actual operating experience.

A. Hazard Analysis

Although there are many definitions of a hazard, for the purposes of this paper, a hazard will be defined as any conditions which has potential to cause an accident. An accident in turn can be defined as a change of operations mode, design or human interface which leads to an unwanted transfer of energy due to lack of barriers or controls which in turn produces injury to persons, property or process. This focuses attention on change, people, energy sources and barriers or controls. Changes can occur in the nature of the work (such as from operation to maintenance), in the environment (from new operating conditions or violent weather conditions) in the machinery (from age, upgrading, or replacement), in the people (from new or transferred persons), in management systems (from reorganization) in procedures (due to design modifications) and in numerous other areas. Accident histories have shown that changing situations are prone to lead to equipment troubles or human error which in turn are likely to trigger accidents.

The hazard analysis addresses the total system from the standpoint of energy sources which can get out of control. The basic logic in conducting this analysis is shown in Figure 8.

Initially, the hazards in a particular system are identified by analyzing engineering and accident information. A human error checklist which is derived from accident/incident experience and human engineering data sources can also be helpful. The operational task is then broken down in a step-by-step procedure, and each step is considered for possibility of human error and probability of a basic hazard leading to an accident. Recommendations are made to eliminate, or control the hazards, to install safety devices, manning devices or to establish special procedures.

Once we have defined the basic hazards and human errors which should be applied in the analysis operation, we consider each of them for each operational phase.

System safety, not only identifies hazards, but also shows the likelihood of their activation and points out the alternative methods available to eliminate them. A potential hazard assessment is usually made using such historical safety data as accident/ incident analyses and safety design, operations and human error checklists. Also, an analysis is made of the plans, concepts and proposed operating modes for the system. These two efforts result in the production of a Preliminary Hazard Analysis. The Preliminary Hazard Analysis list all known hazards with classification as safe, marginal, critical, or catastrophic (9).

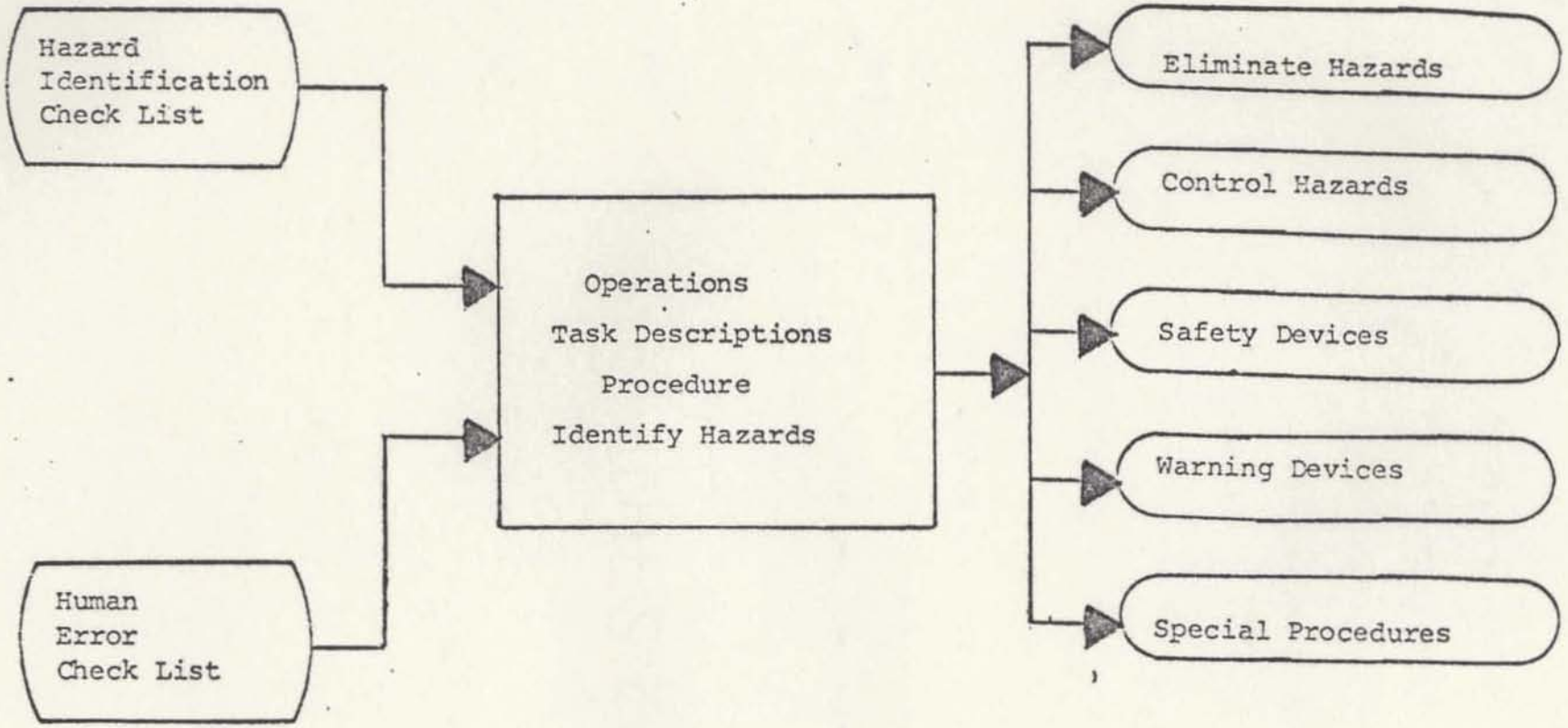


Fig. 8. Basic Logic in Hazard Analysis

Classification of Hazards

Class I.	Safe:	Conditions such that human error, deficiency or inadequacy of design, or equipment malfunction will not result in personnel injury or equipment damage.
Class II.	Marginal:	Conditions such that human error, deficiency or inadequacy of design, or equipment malfunction will degrade system performance or damage equipment, but counteraction or control can be undertaken such that serious injury to personnel or significant damage will not occur.
Class III.	Critical:	Conditions such that human error, deficiency or inadequacy of design, or equipment malfunction will cause personnel injury, serious equipment damage, or will result in a hazard requiring immediate corrective action for personnel or system survival.

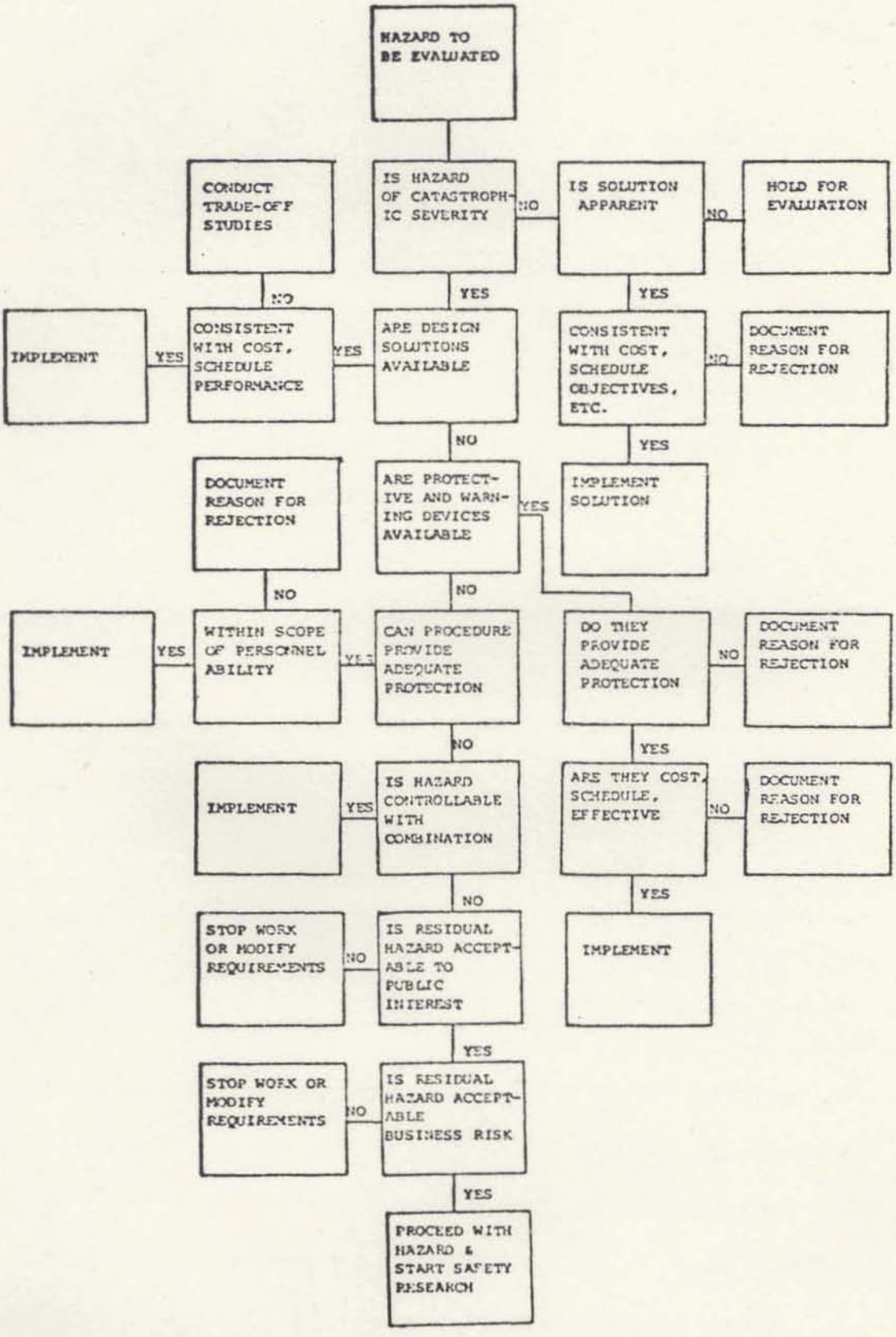


Fig. 9. Hazard Evaluation Logic (10)

Class IV. Catastrophic: Conditions such that human error, deficiency or inadequacy of design, or equipment malfunction will severely degrade system performance and cause subsequent system loss or cause death or serious, irreversible injuries to personnel.

TABLE 2

HAZARD CLASSIFICATION

CLASS	HAZARD	EQUIPMENT DAMAGE	PERSONNEL INJURY
I	SAFE	NONE	NONE
II	MARGINAL	MINOR	NONE
III	CRITICAL	SUBSTANTIAL	*TRANSIENT INJURY
IV	CATASTROPHIC	SYSTEM LOSS	** IRREVERSIBLE INJURY OR DEATH

* Transient Injury - is one from which recovery is effected with no resultant loss of functional capability or shortening of life span.

** Irreversible Injury (residual) - one which is not transient.

As may be seen in Figure 9, the hazard to be evaluated is first checked as to its severity. The hazards are then ranked in the "totem pole" fashion to establish priorities for judgments and actions necessary to eliminating or controlling the hazard. To aid in this ranking, a hazard reduction precedence is used. The

first order of priority, of course, is to eliminate the hazards and the second order to provide safety devices which control the hazards. The third priority is to install warning devices to indicate lack of control and the fourth provides for special control procedures to prevent or amelioriate potential damage.

As development of the system proceeds, the Preliminary Hazard Analysis, by an iterative process, becomes a hazard catalog. This catalog provides a tracking system for each hazard which could have catastrophic or critical consequences. Those hazards which cannot be eliminated or controlled are identified as potential acceptable risks and the logic for these decisions is recorded for each hazard item. The hazard catalog then becomes a risk control document which is constantly reviewed by project management to determine trade-offs in design and operations alternatives.

In Table 3 the general hazards and some of the sub-hazards common to the rail industry, are classified according to the categorization criteria just described.

It has been inferred up to this point that the categorization criteria was carefully selected and documented before hazards are evaluated. In reality the criteria evolved with hazard evaluation efforts as the need for setting priorities was encountered. A similar evolution occurred before the Hazard Evaluation Logic depicted in Figure 9 was specifically documented. This logic provides the well known "hazards precedence sequence" common to

TABLE 3

GENERAL HAZARDS
Common to the Railroad Industry (10)

HAZARD	CLASSIFICATION I	II	III	IV
Personal Injury Incident		X		
Burns/Smoke Inhalation		X		
Tripping/Falling		X		
Electrical Shock			X	
Window Breaking			X	
Fire/Smoke		X		
Undercar		X		
Car Roof		X		
Car Interior			X	
Any of above with unattended car				X
In tunnel or on elevation				X
Collision (includes Excessive Stopping Dist.)				X
With other train(s)				X
Vehicle at Crossing				X
Person or Vehicle on Track				X
Derailment				X
In Yard (low speed)		X		
Revenue Service (moderate speed)			X	
Revenue Service (high speed)				X
Door Opening Underway		X		
Inadvertent Uncoupling				X
In Yard (low speed)		X		
Revenue Service (moderate speed)			X	
Revenue Service (high speed)				X

System Safety efforts. While this portrayal does not add any unique features to the evaluation process, it does provide an ordered reference sequence which assures that each hazard is evaluated consistently and with the same order of consideration.

The hazard evaluation process in Figure 9 is the heart of the System Safety Program under consideration. For this reason a specific example will now be considered on the following page.

The case to be considered involves excessive stopping distance which can clearly be a cause factor in a collision, a hazard of potential catastrophic severity (10). This case involves an apparent failure of a master controller tip-up handle which typically provides the deadman feature on propulsion control equipment. The design concept of the handle requires the operator to hold it in a depressed condition or experience an automatic emergency brake application. With this concept the train is automatically stopped if the operator becomes unconscious or leaves his station. In the cases reported the handle failed to pop up and activate the brake application when released. One of the most likely causes was found to be a missing spring in the mechanism. However, other possible causes such as the assembly technique, quality control in manufacture, and lubrication method were also judged possible. In evaluating and controlling this hazard relative to the logic of Figure 9, it has already been noted that the results of excessive stopping distance could be catastrophic. However, a further consideration was that both the handle and the operator would have to fail simultaneously for potential collision conditions to be present. On this basis, it must be questioned whether the combined protection of the tip-up handle and operating procedures were not sufficient to consider the hazard controllable. The final conclusion arrived at is that protection is adequate but that any simple design improvements should be cut in which could prevent binding, and special quality control attention should be given. In reality, an

improved screw staking procedures was incorporated in the assembly procedure and quality control checks were revised. Additionally, a roll pin was added to the handle design to help prevent an operator from purposely causing its removal with a pencil or other sharp instrument, and thereby defeating the deadman.

B. Logic Tree or Fault Tree Analysis

The Fault Tree Analysis begins by identifying an Undesired Event whose causes are to be traced. Graphically, this event is placed at the top of the page and represents the base of a tree whose branch will be developed and will extend downward. Once the undesired event, also called a Top Event, is specified, it is necessary to identify the immediate causes which directly could cause this top event. Each of these causative events, in turn, can be further broken down into subordinate events. This process is continued until one arrives at basic input events that cannot be broken down further, or for which probability data are available so there is no need to go further. This process creates a diagram which resembles a tree whose branches extend and spread out downward, with each branch terminating in basic input events.

Figure 10 illustrates the diagrammatic arrangement of a fault tree, and Figure 11 identifies and defines the geometric symbolis that are commonly used in fault tree construction (11). It is to be noted that a fault tree consists of three essential elements -- input events, logic gates, and output events. The

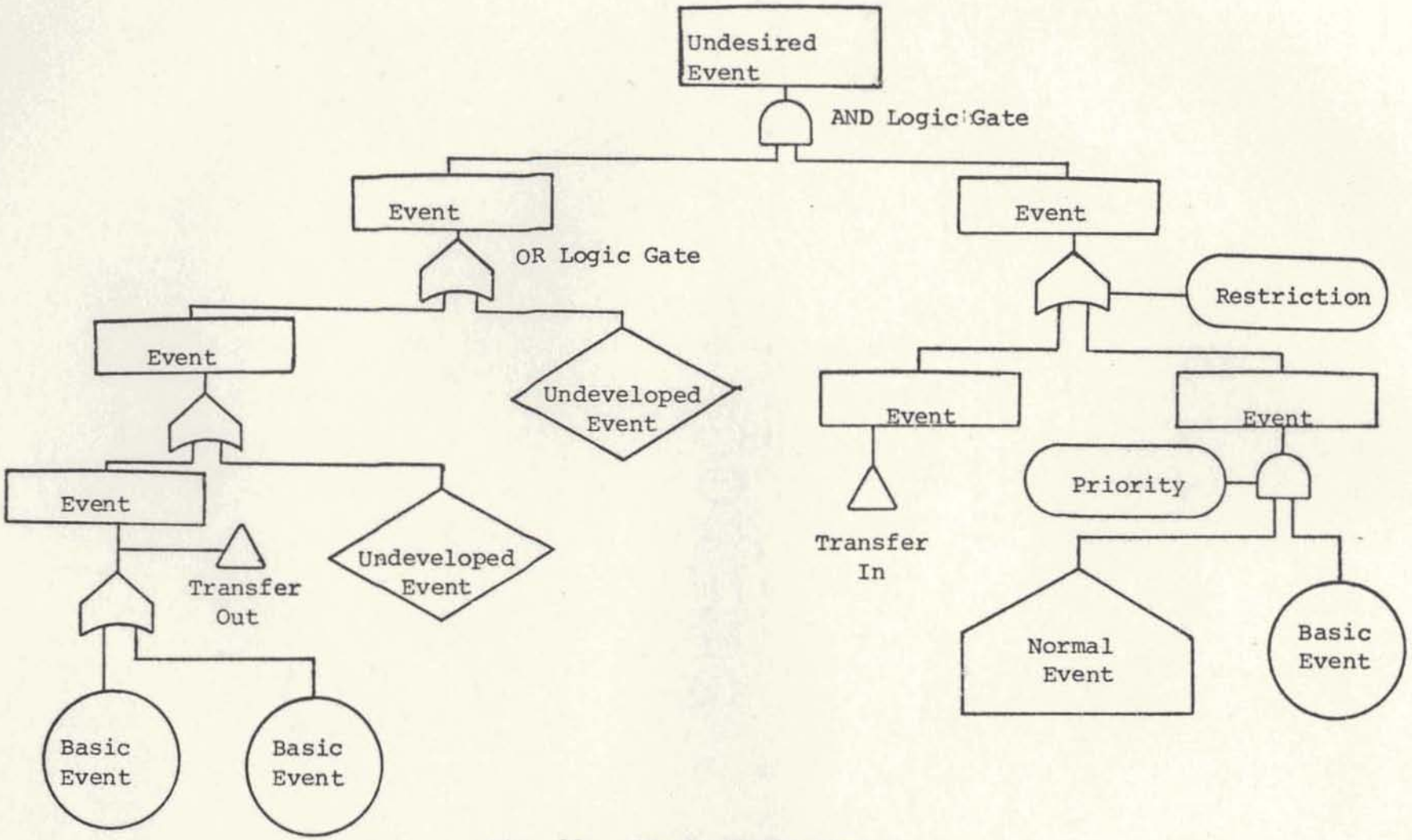
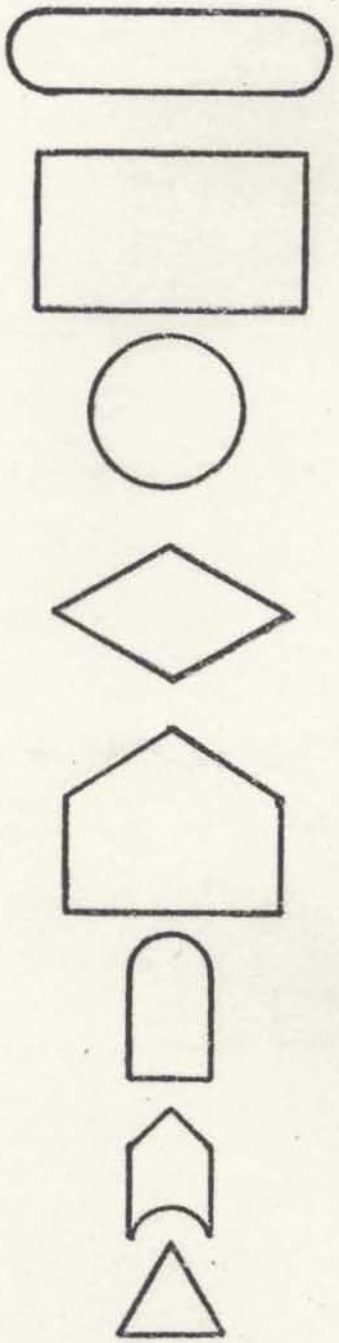


Fig. 10. Sample Fault Tree



Attached to logic gate to specify condition

An event caused by one or more other events which are identified

A basic input event that does not require further development as to causes

An event which is not developed further as to its causes because of lack of information or significance

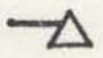
An event which is normal for the system; not a fault or failure per se

AND gate - output event occurs only if all the input events are present

OR gate - output event occurs when one or more of the input events are present

Continuation symbol to identical portion of fault tree

transfer IN



transfer OUT

Fig. 11. Symbols Used in Fault Tree Construction

basic logic gates are of two kinds, namely OR gates and AND gates. If an output event can be caused by one or more input events, either when each acts by itself, or when they act together, these input events pass through an OR gate. On the other hand, if an output event can be caused only when all input events must act in combination, these input events pass through an AND gate.

This concept is illustrated in Figure 12 where the top event is defined as a derailment. Derailment is a hazardous condition which has long been a major concern in the railroad industry. As shown in Figure 12, it can result from a variety of contributing factors and conditions such as track or car defects, or any combination of these coupled with improper operation. A typical example would be excessive speed followed by a wheel slide due to locked wheels, and subsequent derailment while transitioning a worn switch point. Identification of the possible causes is relatively easy for the hazard of derailment. The elimination or correction of these causes can be very difficult.

After the fault tree is completely structured and all branches terminate in basic input events (circles or diamonds), the next step in the analysis is to calculate the probability of occurrence of the top event. The numerical evaluation of a fault tree involves calculating the probability of occurrence of an output event from the known or previously computed probabilities of all input events to the given logic gate. These computations are repeated until the probability of occurrence of the top event

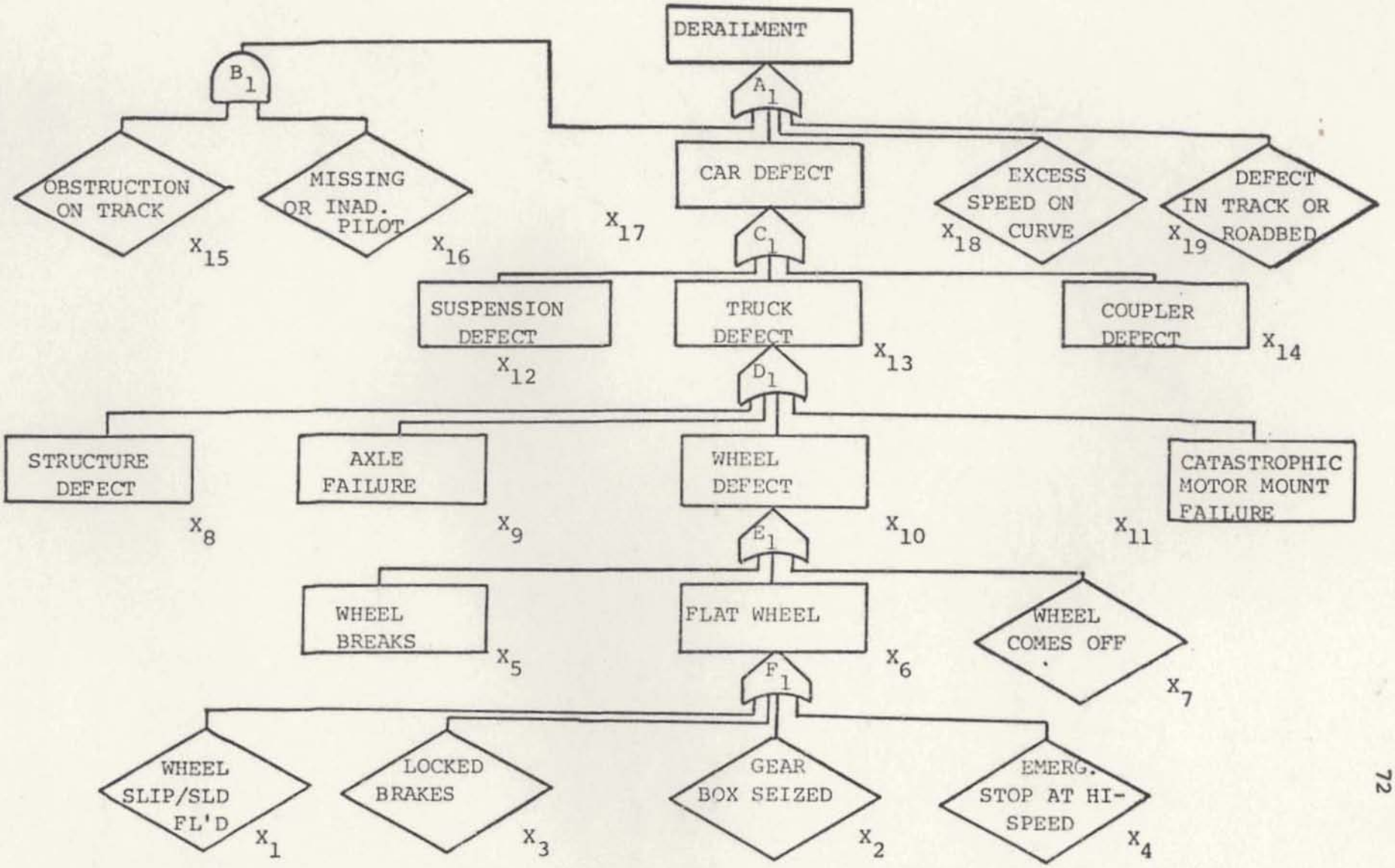


Fig. 12. Fault Tree Analysis of Events or Conditions Leading to a Train Derailment (10)

is determined. Therefore it is necessary to know how the probabilities of the inputs are related to that of the output through the basic logic gates, namely an AND gate or an OR gate.

To evaluate a fault tree manually, it is necessary to perform the following operations (11).

1. Convert the combinationational properties of all the logic elements into Boolean algebraic expressions.
2. Eliminate all redundancies.
3. Evaluate algebraic expressions as probabilities using numerical data for basic input events.

The conversion of the logic diagram into algebraic form must proceed from the bottom up, with every AND gate representing and intersection of the inputs, and every OR gate representing a union of the inputs. The actual algebraic manipulations follow accustomed practice of conventional algebra with an AND gate being analogous to a product and an OR gate being analogous to a sum. The same results would be obtained if one were to use the notation of set theory algebra, namely "u" for a union, or "n" for an intersection.

Boolean algebra (also known as propositional or symbolic algebra) deals only with two states -- yes or no, on or off, success or failure, 1 or 0 -- and is therefore useful for handling the logic gates of a fault tree which may be considered as either open or closed. Since there is almost a one-to-one correspondence between the rules of Boolean algebra and those of set theory, the latter may be used to explain the concepts involved.

In Boolean algebra notation we will be concerned only with two operator symbols. The symbol "*" is used to indicate an intersection of two sets which applies to an AND gate. The symbol "+" is used to indicate the union of two sets which applies to an OR gate. These symbols signify only the above operations and do not have the same meaning as the plus sign or product sign of common arithmetic. However, to the extent that some of the basic laws of common algebra also are valid in Boolean algebra, certain manipulations can be carried out in the accustomed manner. The following laws are valid in Boolean algebra as well as in common algebra (11).

A*B = B*A	Commulative Laws	(1)
A+B = B+A		(2)
A*(B*C) = (A*B)*C	Associative Laws	(3)
A+(B+C) = (A+B)+C		(4)
A*(B+C) = A*B + A*C	Distributive Laws	(5)

In addition to the above, the following laws apply to Boolean algebra and to set theory, but not to common algebra.

A+A = A	(6)
A*A = A	(7)
A+(A*B) = A	(8)
A*(A+B) = A	(9)
A+B*C = (A+B) * (A+C)	(10)

The task of evaluating a fault tree by hand is tedious because the algebraic expressions for intermediate events become progressively longer as one proceeds up the tree to the top event.

The procedure for the manual quantitative evaluation of a fault tree is illustrated below. The example of Figure 12, derailment, is defined as the undesired event. Numerical values for the basic input events were arbitrarily assumed to permit carrying the sample calculations to numerical results.

The followinb Boolean algebraic equations represent the symbolic logic diagram of Figure 12. The sequence shown is from the bottom of the tree upward.

$$X_6 = X_1+X_2+X_3+X_4 \tag{11}$$

$$X_{10} = X_5+X_6+X_7 \tag{12}$$

$$X_{13} = X_8+X_9+X_{10}+X_{11} \tag{13}$$

$$X_{17} = X_{12}+X_{13}+X_{14} \tag{14}$$

$$F_1 = X_6 = X_1+X_2+X_3+X_4 \tag{15}$$

$$E_1 = X_{10} = X_5+X_6+X_7 \tag{16}$$

$$= X_1+X_2+X_3+X_4+X_5+X_7 \tag{17}$$

$$D_1 = X_{13} = X_8+X_9+X_{10}+X_{11} \tag{18}$$

$$= X_5+X_6+X_7+X_8+X_9+X_{11} \tag{19}$$

$$= X_1+X_2+X_3+X_4+X_5+X_7+X_8+X_9+X_{11} \tag{20}$$

$$B1 = X_{15} * X_{16} \tag{23}$$

$$A1 = B1 + X_{17}+X_{18}+X_{19} \tag{24}$$

$$= X_1+X_2+X_3+X_4+X_5+X_7+X_8+X_9+X_{11}X+_{12}X+_{14}X+_{18} +X_{19} + (X_{15}*X_{16}) \tag{25}$$

Equation (25) is the final Boolean equation for the top event A1 in terms of the input events.

In order to evaluate Equation (25) numerically in terms of probability, it is necessary to have probability values for each of the input events. Therefore to proceed with the illustration, a set of assumed values for these events is given in Table 4. Hypothetical values are used because real values are not available in the railroad industry, and if they were the railroads probably would not publish them. Now the probability of the top event can be computed by using Equation (25) and inserting numerical values for the probabilities of the basic input events. Thus

$$A1 = 6.1 \times 10^{-5}$$

This value represents the probability of occurrence of the top event (derailment) based on the assumed values for the input events.

After the probability of occurrence of the top event is determined, it may be desirable to seek ways for reducing this probability by changing some of the input events. To do this most effectively, it is necessary to identify those input events that have the greatest influence on the top event.

TABLE 4

PROBABILITIES FOR INPUT
EVENTS OF FAULT TREE
IN FIGURE 12*

EVENT	PROBABILITY*	EVENT	PROBABILITY*
X_1	$.40 \times 10^{-5}$	X_{11}	$.80 \times 10^{-5}$
X_2	$.50 \times 10^{-5}$	X_{12}	$.20 \times 10^{-5}$
X_3	$.30 \times 10^{-5}$	X_{14}	$.20 \times 10^{-5}$
X_4	$.60 \times 10^{-5}$	X_{15}	2.00×10^{-4}
X_5	$.20 \times 10^{-5}$	X_{16}	$.40 \times 10^{-1}$
X_7	$.10 \times 10^{-5}$	X_{18}	$.60 \times 10^{-5}$
X_8	$.50 \times 10^{-5}$	X_{19}	$.30 \times 10^{-5}$
X_9	$.60 \times 10^{-5}$		

*Values are assumed for purposes of illustration only and have no other significance.

Criticality is a measure of the relative seriousness of the effects of each basic fault, and thus provides a basis for ranking the faults for corrective action priorities. A criticality number for a given basic input event combines the impact this event would have, if it occurred, on the top event, with the likelihood of occurrence of the basic event. The computation of a criticality number therefore involves two steps (11):

1. Assign a value of 1.0 to the probability of a given basic event, while maintaining the probabilities of all other basic events at their real values, and compute the probability of the top event.
2. Multiply the result of step 1 by the actual probability of the given basic event.

The first step yields the probability of occurrence of the top event assuming that the given basic event has already occurred. This result is then modified by the actual likelihood of occurrence of the given basic event.

Criticality numbers are computed in this manner for all basic input events, one at a time, and then the basic events can be ranked according to their criticality as candidates for corrective action.

The manual computation of criticality values can be done by tabular methods. Examples of such computations are given in Table 5 for the same example used previously for illustrating the quantitative evaluation of the fault tree in Figure 12.

In order to calculate the probability of occurrence of the top event, it was previously necessary to derive the algebraic expression for this event, and to compute numbers for each term in the algebraic expression using actual probabilities for the basic input events. To compute the criticality of each basic event, only

TABLE 5

COMPUTATION OF CRITICALITY NUMBERS FOR BASIC EVENTS
IN THE FAULT TREE OF FIGURE 12

Event	Probility of Event	Value of Term* Where Event Occurs	Value of Term if Event Probability=1.0	Probability of Top Event When Event Probability = 1.0	Criticality Value
X_1	$.40X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$4X10^{-6}$
X_2	$.50X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$5X10^{-6}$
X_3	$.30X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$3X10^{-6}$
X_4	$.60X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$6X10^{-6}$
X_5	$.20X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$2X10^{-6}$
X_7	$.10X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$1X10^{-6}$
X_8	$.50X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$5X10^{-6}$
X_9	$.60X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$5X10^{-6}$
X_{11}	$.80X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$8X10^{-6}$
X_{12}	$.20X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$2X10^{-6}$
X_{14}	$.20X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$2X10^{-6}$
X_{15}	$2.0X10^{-4}$	$.8X10^{-5}$	$.40X10^{-1}$	$4.0X10^{-2}$	$8X10^{-6}$
X_{16}	$,40X10^{-1}$	$.8X10^{-5}$	$2.0X10^{-4}$	$2.5X10^{-4}$	$1X10^{-5}$
X_{18}	$.60X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$6X10^{-6}$
X_{19}	$,30X10^{-5}$	$5.3X10^{-5}$	1.0	$10X10^{-1}$	$3X10^{-6}$

*In Equation 25

the following steps are necessary:

1. Recalculate the value of the algebraic term in which the basic event occurs, assuming that its new value is 1.0. If the event probability appears in a term which is a sum, the value of the sum term is automatically 1.0 (and no more than 1.0). If it appears in a product, the value of the term is the same as if the given event is removed from the product.
2. Recalculate the probability of the top event using the result of step 1 (above) for the value of the term in which the given basic event appears.
3. Multiply the result of step 2 (above) by the given probability of the basic event.

The number resulting from the last calculation is a measure of the criticality of the basic event. Those basic events having the highest criticality numbers are the first to be considered for corrective action.

C. Failure Modes and Effects Analysis (FMEA)

The Failure Modes and Effects Analysis is a relatively simple and direct approach for identifying basic sources of failure and their consequences. The method was developed by reliability engineers to determine problems that could arise from malfunctions of hardware. The method is not rigit and can be used for widely differing applications. The primary purpose of the analysis is to identify and remove failures that can cause hazards. However, as a side benefit, the analysis also leads to the identification of failures that are in themselves not hazardous but might affect the reliability of the functioning of a system. The results of such an analysis also may serve as an input to a Fault Tree.

A Failure Modes and Effects Analysis is carried out by filling in a table having column headings such as those shown in Figure 13. Several different formats are shown in this figure to indicate that the method is not rigid and that an analyst may choose his own format on the basis of his experience and needs to make the analysis most useful for the specific application. The column headings shown in Figure 13 are self-explanatory. This type of analysis is generally qualitative only, but not necessarily so. Columns with headings such as Failure Frequency, Probability of Occurrence, Failure Rate, or Mean-Time-Between-Failures, may include either relative terms or numeric values for specific items if such values are available.

The level of detail to which the analysis is carried is a problem that must be resolved by the analyst depending on the purpose

COMPONENT	FAILURE MODE	DIRECT EFFECT	EFFECT ON SYSTEM	HAZARD CATEGORY	RECOMMENDED CHANGE

COMPONENT	OPERATING MODE	FAILURE MODE	HAZARDOUS ASPECT	FAILURE FREQUENCY	HAZARD CATEGORY	REMARKS

ITEM	FAILURE MECHANISM	FAILURE RATE	POSSIBLE HAZARD	HAZARD DURATION	SOURCE OF DATA	CORRECTIVE ACTION

Fig. 13. Sample Formats for Failure-Modes-And-Effects Analysis

of the analysis. For example, if the system being analyzed is a coupling unit for a tanker car, a complete chasis may be considered as a single element in the system, especially if a numerical value is available for the reliability of such a chasis. The analyst would consider all possible modes of failure of the chasis as a whole, and would examine the possible consequences of a failure. At the other extreme, each individual component of that coupling unit might be considered as a separate element of the system.

For an extensive system consisting of a number of subsystems, it may be advisable to divide the system into portions that can be handled conveniently. If the probability or likelihood of occurrence of a failure is of primary interest, the component level to which the analysis is carried out would depend on the level for which reliability data are available. Thus if reliability data are available for an assembly, there would be no need to analyze the failure modes of each component within the assembly.

To carry out a Failure Modes and Effects Analysis, the analyst must have a thorough understanding of all components of the system and of their functions. This understanding may be obtained from drawings, written descriptions, or in the case of small hardware assemblies, by the actual disassembly of the unit into all its components. The elements of the system being analyzed should be listed in a logical sequence so none are omitted.

For each component listed, the analyst must identify and list all conceivable modes of failure or abnormal functioning. He must

then postulate that each such failure or malfunction has indeed occurred and then examine all possible immediate consequences, and the overall effect on the system. Partial failures are not considered. It should be noted that a given component may have more than one mode of failure, and each mode of failure may have more than one effect or consequence. Thus each failure should be considered individually and all consequences of the given failure should be analyzed. The analyst must also attempt to determine how a given failure can be prevented, how critical is each consequence if the failure occurs, and how can criticality of the consequence be reduced.

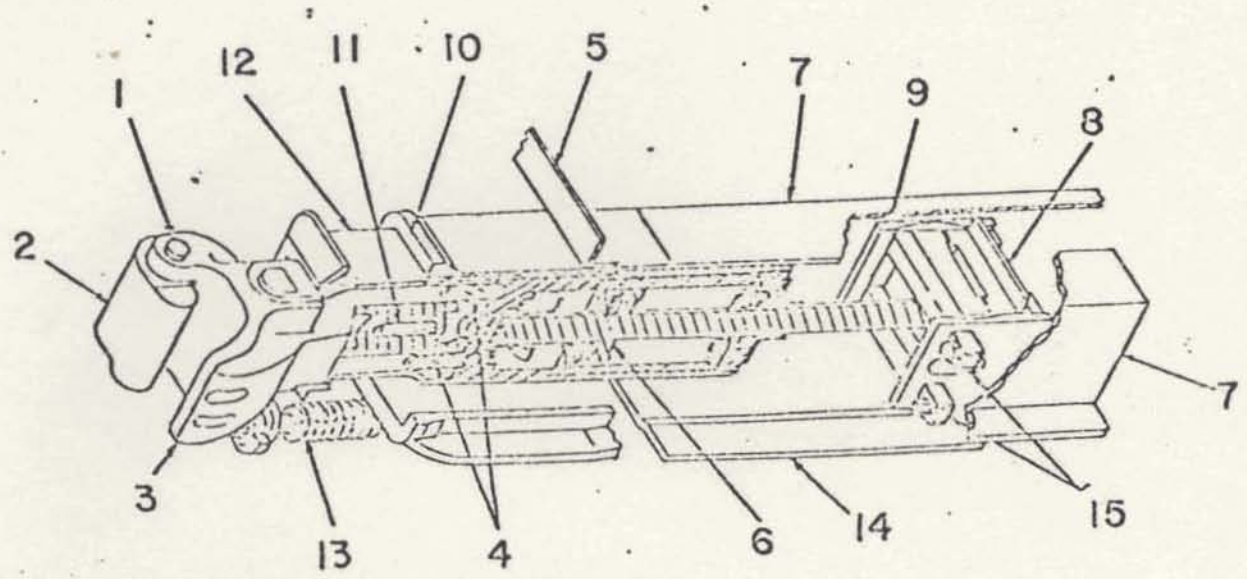
Generally, a Failure Modes and Effects Analysis is first accomplished on a qualitative basis. Quantitative data may then be applied to establish a reliability or failure level for the system or subsystem. Usually four failure modes are considered (12):

1. Premature operation of a component
2. Failure of a component to operate at a prescribed time
3. Failure of a component to cease operation at a prescribed time
4. Failure of a component during operation

In its original usages, Failure Modes and Effects Analysis determined where improvements in component life or design were necessary; and because failure intervals and probabilities were estimated, maintenance periods and requirements could be established.

It has proven effective for both purposes. Deficiencies can be eliminated or minimized through design changes, redundancies, incorporation of fail-safe features, and closer control of critical characteristics during manufacture and use.

While simple and direct, this method also has certain limitations. The most serious is the fact that in dealing with specific failures of individual components, it does not reveal possible failure of the system that may be caused by a combination of events, none of which would be considered hazardous when taken by itself. Similarly, since the method is primarily hardware oriented, it is also unlikely to reveal a system failure that may come about from the combined effect of a component fault, which in itself is not hazardous, but which would create a serious hazard in combination with an abnormal environmental condition, or in combination with a human error. Figure 14 shows a schematic drawing, and list of components of an end-of-car cushioning unit for which an example of Failure Modes and Effects Analysis, is given in Table 6 (13). The analyses are self-explanatory. It should be noted that the blank columns with headings only are shown in this example to indicate that the format is quite arbitrary and can be arranged as desired by the individual analyst.



Component No.	Description
1	Coupler knuckle pin
2	Coupler knuckle
3	Type E coupler head
4	Draft key
5	End sill
6	Hydraulic piston
7	Center sill
8	Back stop plate
9	Rear lug casting
10	Striker casting
11	Coupler key
12	Cushioning unit
13	Restoring mechanism
14	Inspection plate
15	Rear cross key

Fig. 14. End-of-Car Cushioning Unit

TABLE 6

FAILURE MODES AND EFFECTS ANALYSIS OF AN END-OF-CAR CUSHIONING UNIT

ITEM NO.	BASIC CAUSE CONTRIBUTING TO FAILURE	DIRECT EFFECT	EFFECT ON UNIT	HAZARD LEVEL	LIKELIHOOD OF OCCURRENCE	SUGGESTED CORRECTIVE ACTION
1.	Improper composition of material	Faulty Pin	Undesirable strength properties			
2.	Improper composition, heat treatment and handling	Faulty Coupler	Will not couple			
3.	Inoperative restoring mechanism	Coupler Failure	Premature decoupling			
4.	Key material worn, cut, or otherwise failed	Cushioning device is not properly attached	Draft movement is no longer limited			
5.	Sill breaks	Coupler becomes unbalanced	Renders cushioning unit inoperative			
6.	Piston leakage	Reduced compression between coupling units	Loss of pressure regulation			
7.	Cracking	Exposes cushioning unit	Life shortened			
8.	Plate is cracked or broken	Cushioning power is relaxed	Cushioning feature is defeated			
9.	Improper composition of material	Faulty casting	Undesirable strength properties			
10.	Improper composition of material	Faulty casting	Undesirable strength properties			
11.	Key material worn, cut, or otherwise failed	Cushioning device is not properly attached	Unit can move freely			
12.	Piston leakage Inoperative restoring mechanism Faulty striking casting	Coupler failure	Rendered inoperative			
13.	Spring breaks	Spring is partially or completely relaxed	Pressure is reduced			
14.	Improper installation	Components exposed to elements of environment	Premature wearout & replacement of components			
15.	Key loose, cracked, or broken	Unit is not properly secured	Unit can move freely			

D. Probabilistic Cost Analysis

To aid the industry in an attempt to address safety costs, consider the probabilistic behavior of accident systems. It will be useful to classify accident systems into two types, simple and complex (14).

A simple system can be described by a single event rate occurring over elements of time. This rate may be depressed by the expenditure of prevention resources.

A complex system may be described as the interaction of two or more events in the accident causation chain.

It can be shown that if we know the rate of occurrence of an accident event in a given unit of time, t, the probability of no accidents in units of that time, t, may be computed as follows:

$$P(o) = e^{-\lambda t}$$

where λ = event rate

t = number of units of base time, t

The probability of at least one accident can be computed as follows:

$$P(\text{at least 1}) = 1 - P(o)$$

Noting that in rare events, which most simple accident systems are, the probability of at least 1 will compromise the majority of the probability space, the expected cost of an accident can be computed from the mean cost of the particular accident event being examined.

$$E(\text{cost}) = P(1) \times \text{cost}$$

The cost used in this computation will be the sum of the direct and indirect accident event costs.

An example will illustrate this method. Assume that we are concerned with a train derailment resulting in the loss of several freight cars. This occurs once in 10^6 train hours. The accident rate is 1×10^{-6}.

Assuming that within a given company's commercial operations there are 400,000 train hours a year, the probability of at least one train accident in one year is:

$$P(\text{at least 1}) = 1 - P(0)$$
$$= 1 - e^{-(10^{-6})4 \times 10^5}$$
$$= 1 - e^{-.4}$$
$$= .3297$$

The probability of exactly one is:

$$P(1) = \frac{\lambda t e^{-\lambda t}}{1!}$$
$$= .2681$$

The probability of exactly two is:

$$P(2) = \frac{(\lambda t)^2}{2!} e^{-\lambda t}$$
$$= .0536$$

If it is found that the average accident cost associated with an accident of this type is $100,000 then the annual expected cost can be computed as follows:

Expected cost = Event probability x Event cost

$E(c)_1$ = \$26,810 ------- Expected cost of one accident

$E(c)_2$ = \$10,720 ------- Expected cost of two accidents

$E(c)_3$ = \$ 2,144 ------- Expected cost of three accidents

\$39,674 ------- Total Expected Cost (neglecting the cost of more than three accidents)

The expected annual cost of this type of accident may be considered the value of the accident. This is a piece of hard information which will be of significant assistance in reaching a decision as to how much to effectively invest to reduce this type of accident.

The complex accident usually results in much higher costs per accident with lower probabilities. If we examine the more costly of the multiple event activities, the output of the probabilistic examination of the events is a probability density function P(x). The cost of such an accident may also be described by a function C(x). The expected cost of such an accident system may be determined:

$$E(\text{cost}) = \int_{-\infty}^{\infty} P(x)C(x)\,dx$$

The expected value as defined above exists only if the integral is convergent. In addition, the determination of the functions P(x) and C(x) may be difficult in many cases. However, some very simple methods may be used to give a very good approximation of the expected cost.

Assume that we have a diesel engine with three brake control systems. If we lose all three systems, engine control will be lost and a catastrophic accident will result. A brief consideration of the costs of accidents described previously may place the mean cost of such an accident at $20,000,000.

By component analysis and laboratory test, the mean time between failures (MTBF) of the three brake control systems is determined to be the following:

System A -- 10^3 hours

System B -- 3.1×10^3 hours

System C -- 5.4×10^2 hours

Assume eight hour trips and all three systems operative at the beginning of each trip, 1,000 eight hour trips per engine of this type each year, the expected cost may be computed as follows:

$$P(1)_A = 1 - e^{-8/10^3} = .008$$

$$P(1)_B = 1 - e^{-8/3.1 \times 10^3} = .0026$$

$$P(1)_C = 1 - e^{-8/5.4 \times 10^2} = .015$$

$$P(1)_{ABC} = 3.12 \times 10^{-7}$$

$$P(1)_{1\ yr.} = 1 - (1-P(1)_{ABC})^{1000} = 3.12 \times 10^{-4}$$

The probability of an accident of this type occurring in one year is difficult to evaluate as to criticality. However, when the expected cost is computed, the annual value of this type of accident is given necessary visibility

$$E(\text{cost}) = 3.12 \times 10^{-4}(20 \times 10^6) = \$6,240$$

The assumption that P(1) is the probability of exactly one accident, rather than at least one, and that only one may occur will result in an expected cost somewhat lower than the true value. However, for small accident rates the loss in accuracy is small. The lower bound on the expected cost can serve as an action signal. If the value is large enough to signal corrective action, the true value must also be reduced. It is emphasized again that the annual value of accident is a piece of hard information which will assist in the evaluation of the entire safety program.

Discounting Safety Costs

Recalling from the total cost curve of Figure 15, we invest in safety at one point in time and receive our returns from this investment at a later point in time, much as in a normal business investment. We must consider the time value of money in our evaluation of a safety program.

Figure 16 describes ideal results of a normal business investment. It can be seen that a rate of investment over time $t_2 - t_1$, amounting to Capital A will result in return of Capital B over the time $t_y - t_3$. This will be a good investment if the discounted value of B is equal or greater than A at an interest rate equal to the cost of capital to the organization.

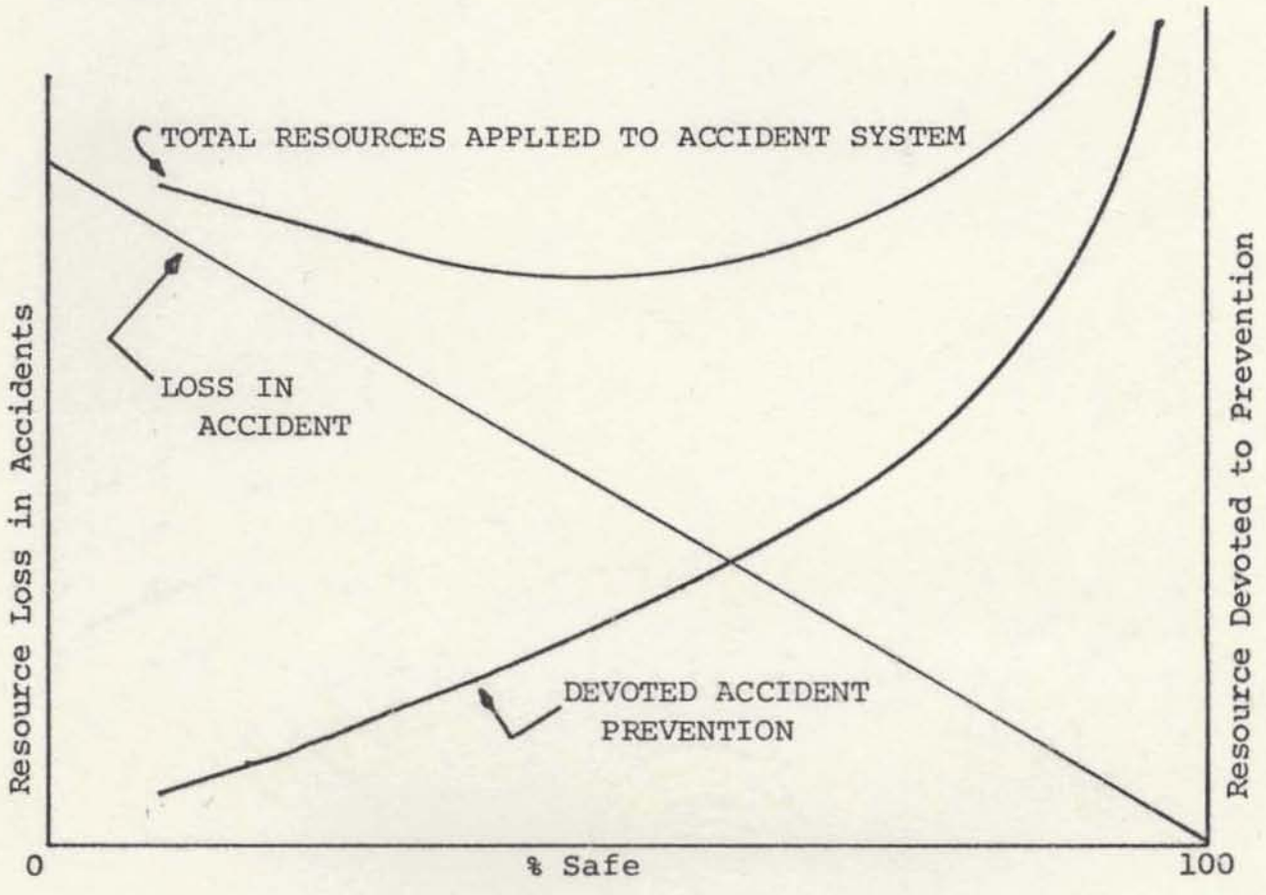
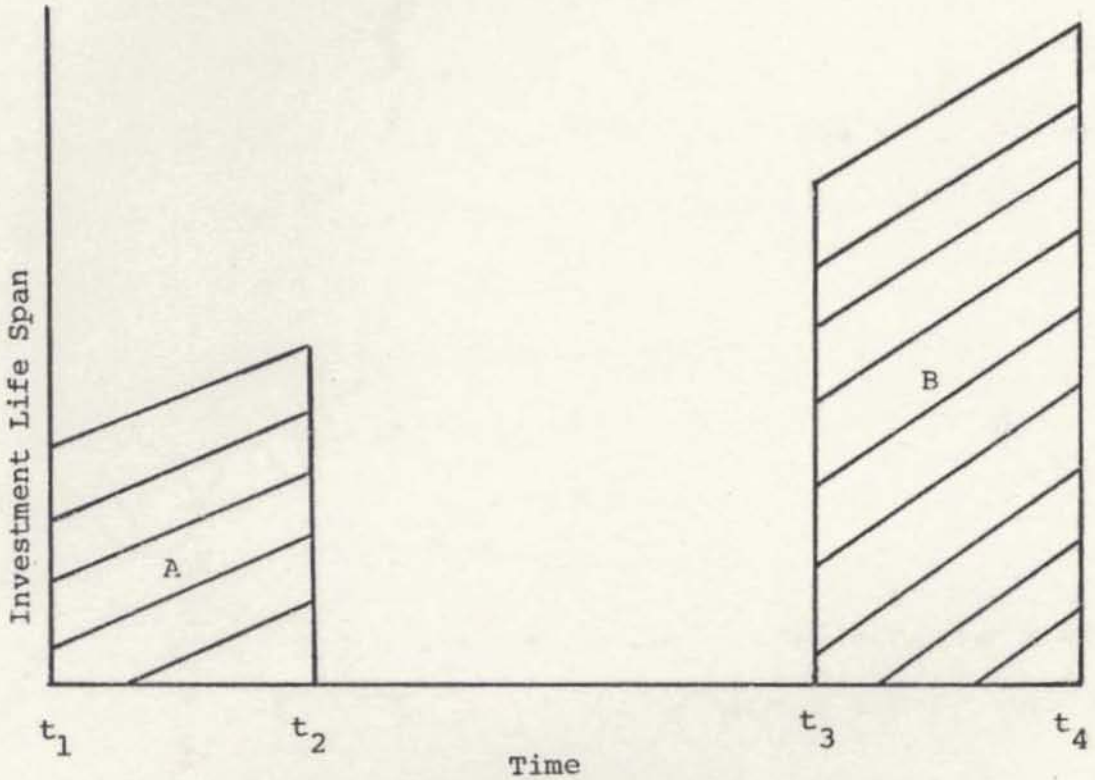


Fig. 15. Total Cost of Safety



$$\sum_{t=t_3}^{t_4} \frac{B}{(1+i)^t} \geq \sum_{t=t_1}^{t_2} \frac{A}{(1+i)^t}$$

Fig. 16. Ideal Results
of A Normal Business Investment

In the case of safety costs, there is no positive return in a business sense. There is however, a reduction in future accident costs. Therefore, a prevention investment is made today to reduce future costs to the company. It is the net present value or the discounted value of all of these costs which must be minimized if we are to operate with our system at the minimum cost point on a total safety resource curve.

There are three conditions which we may consider in an effort to simplify the many variations which will present themselves when attempting to perform such an evaluation.

Case I:

If little is known of the system or its future performance, expected costs of accidents cannot be predicted nor can they be related to prevention costs. In this case, simple bookkeeping may be helpful in locating the system on the safety resource curve of Figure 15. At the conclusion of each fiscal year, prevention and accident costs would be totaled. If the system is new, as it must be, an increasing prevention effort is indicated. The trend of total costs should be down. There may be years in which the costs go up due to the lag between prevention programs and accident reduction. A persistent upward trend in total safety costs would indicate that perhaps the prevention program is too large. This cannot be the case if the prevention program is a small fraction of the accident costs. Inflation can be a problem here and must be removed from the

computations in this method of analysis. This technique is analogous to the federal and state methods of financial accounting in which the books are closed at the end of the fiscal year with no effort to account for the return to society from the resources invested during the current year. Figure 17 depicts this method of safety value analysis.

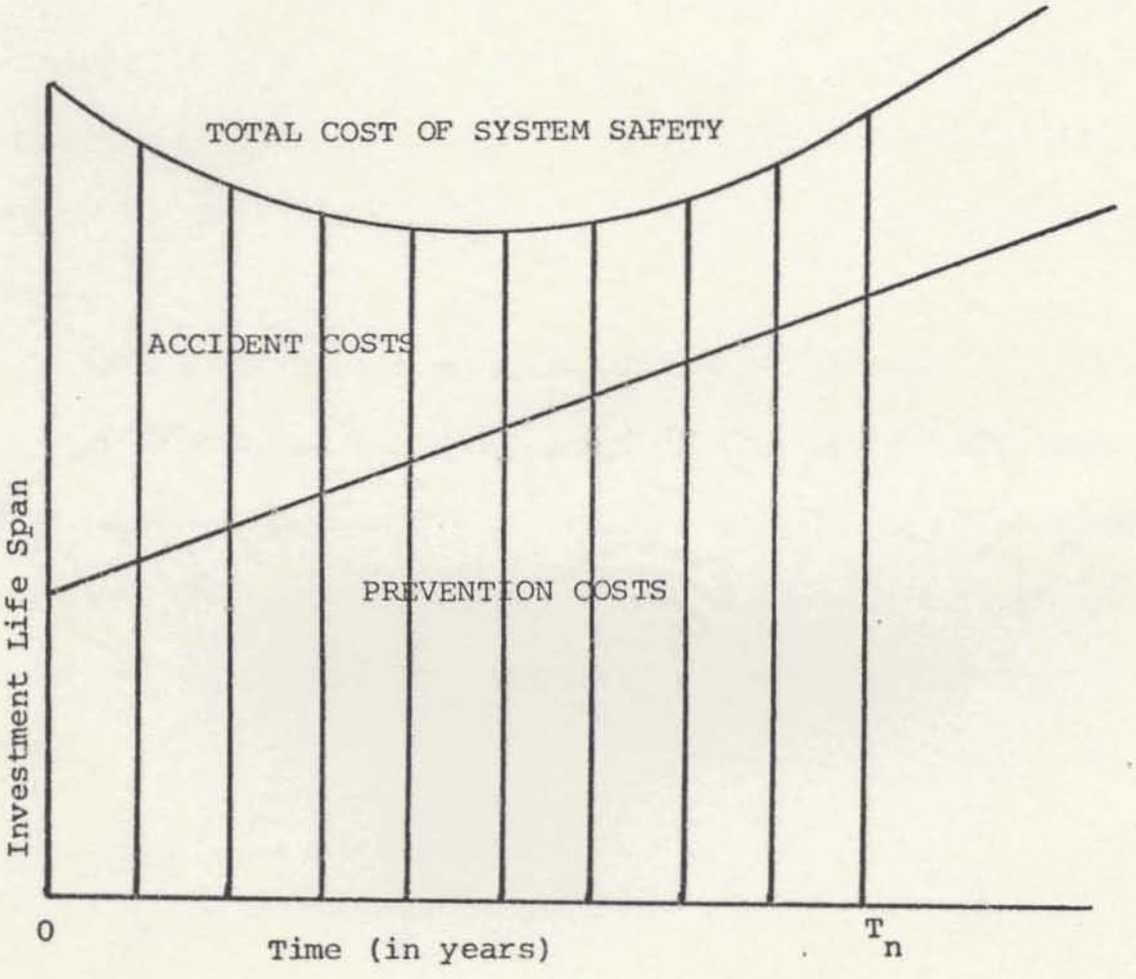


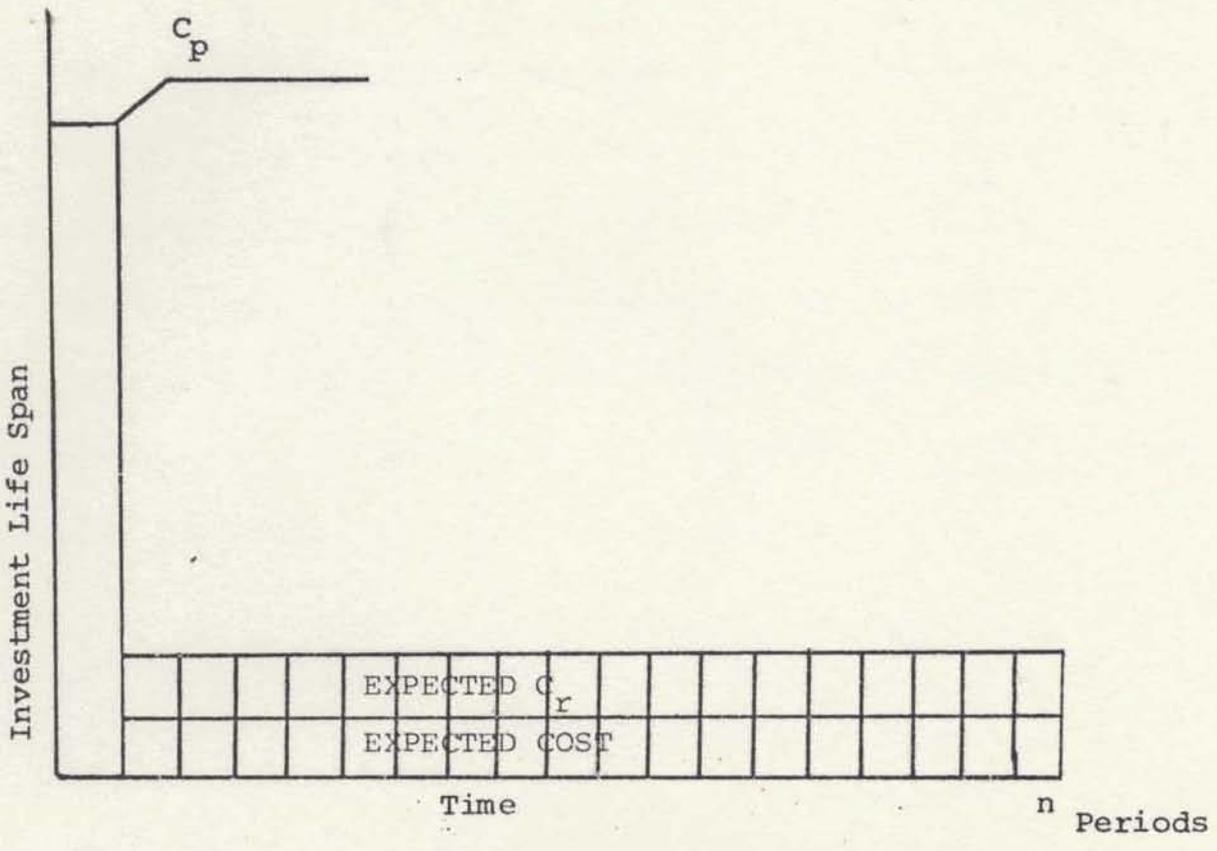
Fig. 17. Federal and
State Methods of Financial Accounting

Case 2:

Frequently specific safety projects can be identified. These projects require a large investment of resources at a point in time. It is hoped that future reduction in accident costs will in some way compensate for this investment.

An attractive attribute of using dollars to measure the value of a safety project is that from the point of view of society, their value remains linear relative to total worth. It is, therefore, possible to separate specific projects from the total system safety analysis.

Figure 18 illustrates this method of analysis. It can be seen that if the discounted value of the future accident cost attributable to the project is equal to or greater than the initial investment cost of the project, the project is justifiable in that it will result in reduced total safety cost attributable to this system.



$$C_p \leq \sum^{n} \frac{E(Cr)}{(1+i)^n}$$

where:

C_p = cost of prevention or cost of this project

E(Cr) = expected accident cost reduction

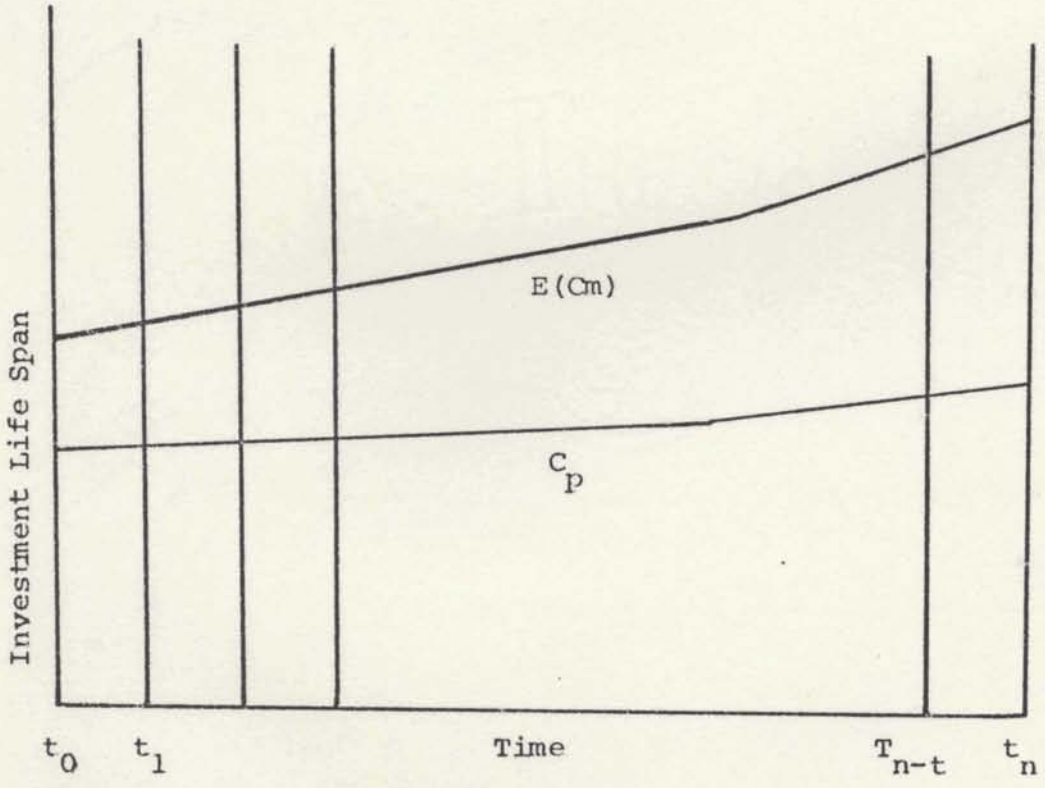
i = interest rate, usually the cost of capital for the project

n = number of periods to the planning horizon for this project

Fig. 18. Cost of a Specific Project

Case 3:

The third and more general case of system safety value analysis is the condition of continuous expenditure to the planning horizon for accident prevention. This expenditure should be accompanied by a corresponding reduction in the expected cost of accidents. The discounted value of the cost reduction must be greater than the discounted value of the prevention costs. Figure 19 depicts this method of safety value analysis.



$$\sum_{t_0}^{t_{n-1}} \frac{C_p}{(1+i)^t} \leq \sum_{t_1}^{t_n} \frac{E(C_r)}{(1+i)^t}$$

Fig. 19. Discounted Value of Prevention Cost

The safety department continually finds itself in competition for company resources in the process of implementation of their safety programs. Traditionally the method of "selling" their program is to invoke the spector of a catastrophe or to insist that the system requires a greater degree of safety. In this situation, competing against well documented and quantifiable demands for resource application to other elements of the system, the safety department is at a distinct disadvantage.

VII. CONCLUSION

In conclusion, it should be reiterated that the railroad industry has a history of pursuing and solving safety problems. The extreme magnitude and complexity of the total American railroad system, makes identification and control of all potential hazards an extremely involved task. While it is not possible to examine the American railroad system in the concept stage, it is however, now possible to analyze incremental changes in subsystems for their potential impact on the entire system. Implementation of appropriate changes within the existing system can and will result in control and elimination of hazards in the railroad industry.

A comprehensive system safety program is defined as the selection and implementation of the mechanisms necessary for achieving and maintaining an optimum level of safety in the operations of the railroad industry. It encompasses the total definition of policy, organization, operational control, evaluation, and corrective action - considering the railroad capability of the nation as a system and safety as a principal objective of that system.

By utilizing the systematic approach to safety, railroad accidents can be predicted and analyzed before they occur. They can then be prevented by taking the action necessary to eliminate

or control the hazards which lead to accidents. System safety analysis methods will identify possible hazards. Risks will not be assumed unknowingly. Those risks which are assumed will be those that have been identified, and in which a management decision has been made to accept them. This approach avoids crises by foreseeing them.

The benefits to be derived from the system safety approach go far beyond the prevention of an accident. The resources allocated for system safety are well spent. In addition to the large sums needed to settle accident claims, make repairs to the system and restore the environment, consideration must be given to the value of the operating company's reputation, image, and future business potential. One accident that could have been avoided can cost many times the price of an effective analysis effort.

A number of the accidents investigated by the Federal Railroad Administration revealed the existence of hazards that were activated into accidents. System safety analysis would have made these hazards known and given management a chance to correct them before the accident occurred.

The system safety organization may be defined as the group of people responsible for establishing, managing and performing the overall system safety program. This definition places no constraints upon the size or the character of the safety organization. Furthermore, the definition is equally applicable to system safety organizations that may be identified as a single entity and to those

that are widely diffused and cannot be represented on a conventional organization chart as a single entity. Although one cannot prescribe a unique system safety organization on a prior basis, the functions and responsibilities of all persons associated with establishing policy or implementing any aspects of the safety program should be clearly established.

The System Safety Programs presented in the hypothetical model is one approach to utilizing the principles of System Safety as developed and used in the Aerospace Industry. It is believed to be an effective approach in that it addresses the basic goal of accident prevention through the judicious application of hazard identification techniques such as fault trees, evaluates the hazards using qualitative decision tree logic, and assures the implementation of elimination or control measures consistent with the hazard precedence sequence expounded as an integral part of system safety. On the other hand, it is designed to take full advantage of rail industry experience accumulated by owners, builders, and the using public.

It is obvious that rail transit hazards having the potential for catastrophic results are collision and derailment which can result from failures of critical car systems, wayside equipment, the running rail, operating personnel or any combination. Therefore, the prevention of collisions or derailments will best be achieved from the car standpoint by enhancing the failsafety of contributing systems. At the same time, continued application of "lessons learned" from accidents which have happened must be made. The

hazard associated with mixing different types of car construction and brake systems in the same service is an example of one such lesson learned.

Hazards resulting individually in much less severe consequences also must be given continued attention since greater frequencies of occurrence can easily reach a high cumulative severity. To this end the interfaces between the car and its environment including the using public must be evaluated in the interests of safety enhancement.

If the foregoing safety actions are applied, using the application of System Safety principles described or ones similar to them, rail transit will continue to be a leader as a safe mode of transportation and will even improve as rail transit expands.

The objective of this thesis was to explore and consider such system safety programs and techniques that would enhance the accident and fatality problem in the rail industry. It is recognized that these initial efforts only serve to open the door and that much more comprehensive research is needed.

FOOTNOTES

1. "Statement of Asaph H. Hall, Acting Federal Railroad Administration. Before the Senate Appropriations Subcommittee on Transportation, on Fiscal Year 1976 Appropriations to the Department of Transportation, May 8, 1975: Supplemental Statement." (Washington, D.C.: American Railroad Association, n.d.), 33p. (Mimeographed).

2. "1974 Annual Report by the President to the Congress on The Administration of the Federal Railroad Safety Act of 1970." (Washington, D.C.: American Railroad Association, n.d.), 64p. (Mimeographed).

3. "Derailments Up As Companies Defer Maintenance," Orlando (Fla.) Sentinel Star, 14 January 1975, sec. A, p. 15. A. M. edition.

4. National Transportation Safety Board. Special Study: A Systematic Approach to Pipeline Safety (Washington, D.C.: NTS B-PSS-72-1, 1972), p. 2.

5. Vernon L. Grose, "System Safety in Rapid Rail Transit," 1971, Tustin Institute of Technology, Santa Barbara, California, p. 3.

6. Sherman C. Blumenthal, Management Information Systems: A Framework for Planning and Development (Englewood Cliffs, New Jersey: Prentice-Hall, 1969), p. 57.

7. Robert G. Murdock and Joel E. Ross, Information Systems for Modern Management (Englewood Cliffs, New Jersey: Prentice-Hall, 1971), p. 264.

8. Robert G. Murdock and Joel R. Ross, Information Systems for Modern Management (Englewood Cliffs, New Jersey: Prentice-Hall, 1971), p. 168.

9. Sol W. Malasky, System Safety Planning/Engineering/ Management (Rochelle Park, New Jersey: Prentice-Hall, 1974), p. 11.

10. Lorne L. McMonagle, "Accident Prevention in Rail Transit," in International System Safety Symposium. Technical Summary, Volume IIA, ed. System Safety Society (Denver, Colorado: 1973), p. 62.

11. Alexander Goldsmith, Guide to System Safety Analysis in the Gas Industry (Arlington, Virginia: American Gas Association, n.d.), p. 27-115.

12. Willie Hammer, Handbook of System and Product Safety (Englewood Cliffs, New Jersey: Prentice-Hall, 1972), p. 149.

13. Railroad Educational Bureau, Railroad Cars (Chicago, Illinois: Simmons-Boardman, 1973), chart.

14. Harold E. Roland, "System Safety Management Through Value Analysis," in International System Safety Symposium. Technical Summary, Volume IIA, ed. System Safety Society (Denver, Colorado: 1973), p. 149.

BIBLIOGRAPHY

Blumenthal, Sherman C. Management Information Systems: A Framework for Planning and Development. Englewood Cliffs, New Jersey: Prentice-Hall, 1969. 218p.

"Derailments Up As Companies Defer Maintenance." Orlando (Fla.) Sentinel Star, 14 January 1975, sec. A, p. 15, A.M. edition.

Goldsmith, Alexander. Guide to System Safety Analysis in the Gas Industry. Arlington, Virginia: American Gas Association, n.d. pp. 27-115.

Hammer, Willie. Handbook of System and Product Safety. Englewood Cliffs, New Jersey: Prentice-Hall, 1972. 351p.

Malasky, Sol W. System Safety Planning/Engineering/Management. Rochelle Park, New Jersey: Hayden Book Company, 1974. 331p.

McMonagle, Lorne L. "Accident Prevention in Rail Transit." in International System Safety Symposium. Technical Summary, Volume IIA, pp. 62-95. Edited by System Safety Society. Denver, Colorado: 1973.

Murdock, Robert G., and Ross, Joel E. Information Systems for Modern Management. Englewood Cliffs, New Jersey: Prentice-Hall, 1971. 570p.

National Transportation Safety Board. Special Study of Rapid Rail Transit. Washington, D.C.: NTSB-PSS-71-1, 1972. p.15.

National Transportation Safety Board. Special Study: A Systematic Approach to Pipeline Safety. Washington, D.C.: NTSB-PPS-72-1, 1972. p.13.

"1974 Annual Report by the President to the Congress on the Administration of the Federal Railroad Safety Act of 1970," Washington, D.C.: American Railroad Association, n.d. p. 64. (Mimeographed).

'Perspective for System Safety.' in "NASA Government-Industry System Safety Conference Report," pp. 3-9. Edited by Willard J. Smith. Greenbelt, Maryland: 1971. (Mimeographed).

Railroad Educational Bureau. Railroad Cars. Chicago, Illinois: Simmons-Boardman, 1973. chart.

Rect, J. L., "System Safety Analysis - A Modern Approach to Safety Problems," National Safety News, (December 1965): 58p.

Roland, Harold E. "System Safety Management Through Value Analysis." in International System Safety Symposium. Technical Summary, Volume IIA, pp. 6-25. Edited by System Safety Society. Denver, Colorado: 1973.

Santa Barbara, California. Tustin Institute of Technology. Vernon L. Grose, "System Safety in Rapid Rail Transit," 1971.

"Statement of Asaph H. Hall, Acting Federal Railroad Administrator, Before the Senate Appropriations Subcommittee on Transportation on Fiscal Year 1976 Appropriations to the Department of Transportation May 8, 1975: Supplemental Statement." Washington, D.C.: American Railroad Association, n.d. 33p. (Mimeographed).

"System Safety Analytical Techniques." in Safety Engineering Bulletin No. 2, p. 3-7. Edited by Electronic Industries Association. Washington, D.C.: 1971.

"System Safety Spreads Into Industry." Business Week (July 17, 1971): 57 plus.

United States Army Munitions Command Headquarters. Safety Hazards Analysis. Dover, New Jersey: USA MUCOM Regulation No. 385-22, 1971. p. 12.

United States, Department of Defense. "System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for." Washington, D.C.: MIL-STD-882, 1969.

United States, Department of Transportation. Federal Railroad Administration. Office of Safety. "Summary and Analysis of Accidents on Railroads in the United States," Accident Bulletin, No. 142 (1973): p. 21-41.